目　　录

一、初等数论……………………………………………2
1．整数的整除性……………………………………2
2．最大公因数和最小公倍数………………………5
3．不定方程…………………………………………7
4．同余 ……………………………………………12
5．完全剩余系 ……………………………………18
6．连分数 …………………………………………21
7．素数分布 ………………………………………26
8．关于完全数和麦森素数 ………………………31
二、解析数论……………………………………………33
1．三角和 …………………………………………34
2．古典筛法 ………………………………………35
3．大筛法 …………………………………………38
4．大筛法在证明哥德巴赫猜想中的应用 ………41
5．黎曼ζ函数 …………………………………………45
6．狄利克雷特征 …………………………………48
7．狄利克雷L函数 ………………………………50
三、代数数论……………………………………………53

数论是研究数的性质的一门科学，是数学的一个分支学科.

人类对数论的研究，渊源久远. 早在古希腊时代，就已取得了许多成果. 欧几里得(Euclid)的《原本》一书中，就记有素数有无限多个(及其证明)、整数的因数分解、欧几里得除法（即辗转相除法，用以求两个数的最大公因数)、关于完全数的一个著名定理等；作为古希腊的成就，还有寻求素数的埃拉托斯散(Eratosthenes)筛法，阿基米得(Archimedes)对不定方程所作的研究等. 亚历山大里亚时代的丢番图(Diophantus)曾对不定方程进行了深入的研究. 当然，在数论的发展史上，更应该提到的是法国业余数学家费马(P. S. de Fermat)、德国数学家高斯(C. F. Gauss)以及狄利克雷(P.G. Dirichlet).

我国古代，在数论方面也有极其光辉的成就. 例如商高定理(勾股定理)、孙子定理(被西方人称为“中国剩余定理”)都为世人所瞩目. 近代，我国数学工作者在解析数论、丢番图方程、一致分布等方面，都作出了重要贡献. 特别是华罗庚教授在三角和估计以及堆垒数论方面，成就卓著. 近三十多年来，我国的数论研究队伍中新人辈出，在哥德巴赫(C. Goldbach)问题、算术级数中的最小素数问题、L 函数的零点问题以及三角和的估计等问题

上，更进一步获得了许多优秀的成果.

数论按照所运用的研究方法的不同，又分为初等数论、解析数论、代数数论、几何数论等，下面择要加以介绍.

一、初等数论

初等数论是仅仅利用初等数学的方法，而不借助于其他数学工具，去研究整数的性质. 它主要包括：整除性、不定方程、同余式、连分数等.

1. 整数的整除性

大家知道，整数对于加法、减法、乘法是封闭的，即：整数加整数、整数减整数、整数乘以整数，其结果仍然是整数. 但是，整数除以整数就不一定得到整数了. 于是，产生了数论的一个基本问题——研究一个整数能否被另一个整数整除的问题：

如果三个不为零的整数 a、b、c，满足

$$a=b\cdot c,$$

我们就说"a 能被 b 整除"（或"a 能被 c 整除"），记为$b|a$（或 $c|a$），并说"b（或 c）是 a 的一个**因数**"；而且，当 b 或 c 不为 a 或 1 时，称 b（或c）是 a 的一个**真因数**. 否则，就说"a 不能被 b（或 c）整除"，记为 $b\nmid a$（或 $c\nmid a$）. 我

们把这个基本问题，称为**整数的整除性**.

我们以 $[\alpha]$ 表示不超过数 α 的最大整数. 例如，$[3]=3$，$[\sqrt{2}]=1$，$[\pi]=3$，$[-\sqrt{2}]=-2$，$[-4.5]=-5$.那么，显然成立下面的不等式：

$$[\alpha]\leqslant\alpha<[\alpha]+1.$$

对于两个整数 a 和 b（其中 $b>0$）的商，有

$$\left[\frac{a}{b}\right]\leqslant\frac{a}{b}<\left[\frac{a}{b}\right]+1,$$

即

$$0\leqslant a-b\left[\frac{a}{b}\right]<b.$$

于是，我们有

$$a=\left[\frac{a}{b}\right]b+r,\qquad \text{这里 } 0\leqslant r<b.$$

因此，给定任意两个整数 a、b（其中 $b>0$），必存在整数 q、r，使

$$a=qb+r,\qquad \text{这里 } 0\leqslant r<b.$$

当 $r=0$ 时，就是前面所说的"b 能整除 a"；当 $r\neq0$ 时，即是"b 不能整除 a".

为了研究整数的整除性，人们把正整数分为如下三类：

（1） 1；它只有 1 为其因数；

（2） p；它只有 1 和 p 为其因数，即 p 大于 1 且无真因数；

（3） n；有真因数.

我们把上述第二类数叫做**素数**（在有些书上也称之为**质**

数)，把上述第三类正整数叫做**复合数**（有些书上也称之为**合数**）. 显然，大于 2 的偶数必有真因数 2，都是复合数.

把素数按照大小进行排列，可以得到下面的数列(通常称为**素数列**)：

$$2,3,5,7,11,13,17,19,23,29,31,37,\cdots\cdots.$$

在古希腊，欧几里得就已证明了素数有无穷多个，他采用了反证法：假设素数只有有限个，不妨设这有限个不同的素数是 p_1、p_2、……、p_n；我们来考察整数 $a=p_1\cdot p_2\cdot\cdots\cdots\cdot p_n+1$，依假定，$a$ 显然异于任一素数，因而是一个复合数；于是，根据复合数的定义，a 应该有一个素因数 p，但 $p\nmid 1$ 而 $p|p_1\cdot p_2\cdot\cdots\cdots\cdot p_n$，可知 $p\nmid a$，这就和前面导出的 p 是 a 的素因数产生了矛盾，究其原因，是假设了素数只有有限个是错误的，这就证明了素数有无穷多个.

关于素数分布的研究，是很有趣，又很困难的. 本书在下面的章节里还将讲到.

算术基本定理 每一个大于 1 的整数 n，可唯一地表为

$$n=p_1^{a_1}\cdot p_2^{a_2}\cdot\cdots\cdots\cdot p_k^{a_k}$$

的形状，这里素数 $p_1<p_2<\cdots\cdots<p_k$，而 a_1、a_2、……、a_k 是大于 0 的整数.

这个定理的证明，仅用简单的初等方法就可完成，但定理的结论是非常深刻的. 它反映了素数在整数中的基本作用，揭示了整数的一个基本性质——积性.

2. 最大公因数和最小公倍数

如果 a、b 是非零整数，而整数 q 同时是 a、b 的因数，我们便把 q 叫做 a、b 的**公因数**.

显然，q 的绝对值必不大于 a、b 的绝对值的最小者：

$$|q|\leqslant\min\{|a|,\ |b|\}.$$

上式表明，两个非零整数的公因数必只有有限多个．于是，其中一定有一个最大的；我们把 a 和 b 的所有公因数中的最大一个公因数 d，叫做 a 和 b 的**最大公因数**，记作 $d=(a,\ b)$.

已知两个非零整数 a 和 b，怎样求出它们的最大公因数呢？当然，可以利用上面的算术基本定理；但是，更简单的办法是采用辗转相除法，这一方法最早见于欧几里得的《原本》(公元前三世纪)，我国古算书《九章算术》(约成书于东汉初年，公元一世纪)也记有这一方法.

用辗转相除法求两个非零整数的最大公因数的具体步骤如下：(不妨设 a 与 b 都是正整数，且 $a>b$)

先用 b 除 a，得到正整数 q_1，使

$$a=q_1b+r_1. \qquad (0\leqslant r_1<b)$$

若 $r_1=0$，则由 $a=q_1b$ 知 a 与 b 的最大公因数是 b. 若 $r_1\neq0$，由 $0<r_1<b$，可再以 r_1 除 b，于是又可得正整数 q_2 和非负整数 r_2，使

$$b=q_2r_1+r_2. \qquad (0\leqslant r_2<r_1)$$

以$(a,\ b)$表 a 与 b 的最大公因数，则可知

$$(a, b)=(b, r_1).$$

当 $r_2=0$ 时，可知$(a, b)=(b, r_1)=r_1$. 若 $r_2\neq0$，则$0<r_2<r_1$，再以 r_2 除 r_1，得正整数 q_3 和非负整数 r_3，使

$$r_1=q_3r_2+r_3. \qquad (0\leqslant r_3<r_2)$$

于是，当 $r_3=0$ 时，有$(a, b)=(b, r_1)=(r_1, r_2)=r_2$. 若 $r_3\neq0$，则由 $0<r_3<r_2$，又可再以 r_3 除 r_2，……. 这样继续辗转相除，由于 $b>r_1>r_2>r_3>\cdots\cdots$且各 r_i(这里 $i=1,2,3,\cdots$)皆是非负整数，则一定存在一个正整数 n，使经过$n+1$ 次辗转相除后，有 $r_{n+1}=0$ 但 $r_n\neq0$. 这时，就可得到$(a, b)=r_n$.

这就通过辗转相除，求出了 a 和 b 的最大公因数.

两个非零整数的最大公因数的性质，主要有：如果$(a, b)=d$，则存在整数 m、n，使

$$ma+nb=d; \qquad (1)$$

这里的整数 m 和 n，可由辗转相除法求得$(a,b)=r_n$ 后，逐次向上一算式回代而得.

如果$(a, b)=1$，我们称 a 和 b 是**互素的**. 当然，互素的整数中，可以不一定有素数. 例如$(25,26)=1$，但25 和 26 都是复合数.

对于非零整数 a、b，如果 m 同时是 a、b 的倍数，我们便把 m 叫做 a 和 b 的**公倍数**.

可以看出，a 和 b 的公倍数有无穷多个. 例如，它们的积 ab 即是它们的一个公倍数，而这一乘积的任意倍数都是它们的公倍数. 我们把 a 和 b 的公倍数中的最小的一个数 M，叫做 a 和 b 的**最小公倍数**，记作 $M=\{a,b\}$.

当然，两个非零整数的最小公倍数，也可以利用上面的算术基本定理而求得．

下面，我们来证明关于最大公因数和最小公倍数之间的一个结果：正整数 a 与 b 的乘积，可以表示成

$$ab=(a,\ b)\cdot\{a,\ b\}. \tag{2}$$

证明 因 ab 为 a 与 b 的公倍数，而$\{a,\ b\}$为 a 与 b 的最小公倍数，故存在正整数 q，使

$$ab=q\cdot\{a,b\};$$

从而$\dfrac{a}{q}=\dfrac{\{a,\ b\}}{b}$、$\dfrac{b}{q}=\dfrac{\{a,\ b\}}{a}$；而$\dfrac{\{a,b\}}{b}$与$\dfrac{\{a,b\}}{a}$皆为正整数，所以 $q|a$、$q|b$，即 q 为 a、b 的公因数．又设 g 为 a、b 的任一个公因数，令 $m=\dfrac{ab}{g}$．由于$\dfrac{a}{g}$及$\dfrac{b}{g}$都是正整数，又 $m=a\left(\dfrac{b}{g}\right)=b\left(\dfrac{a}{g}\right)$，故 m 是a 和 b 的公倍数，从而$\{a,\ b\}|m$，即$\dfrac{m}{\{a,b\}}$是一个正整数．又由

$$\frac{m}{\{a,b\}}=\frac{ab}{g\left(\dfrac{ab}{q}\right)}=\frac{q}{g},$$

故$\dfrac{q}{g}$也是正整数，即 $g|q$．由 g 的任意性，可知 $q=(a,b)$，这就证明了(2)式成立．

3．不定方程

如果未知数的个数多于方程的个数，这样的方程叫

做不定方程. 例如,方程

$$ax+by=c,$$

$$ax+by+cz=d,$$

$$ax^2+bxy+cx+dw=0,$$

等等,都是不定方程.

研究整系数不定方程的整数解，是数论中饶有趣味的问题之一. 五世纪末，我国古代数学家张丘建曾编写了一部《算经》，书中提出了一个不定方程问题——世界数学史上有名的“百鸡问题”:

鸡翁一，值钱五. 鸡母一，值钱三. 鸡雏三，值钱一. 百钱买百鸡，问鸡翁、母、雏各几何?

(用现在的白话文来说，就是:每一个大公鸡的售价是五个钱,每一只母鸡的售价是三个钱,每三个小鸡的售价是一个钱;现有 100 个钱,想买 100 只鸡,问公鸡、母鸡和小鸡各应买几只?)

假设用 x、y、z 分别代表买公鸡、母鸡和小鸡的数目,就得到下面的两个方程

$$\begin{cases}5x+3y+\dfrac{z}{3}=100,\\ x+y+z=100.\end{cases}$$

由这两个方程,我们得到

$$\begin{aligned}200&=300-100\\&=3\left(5x+3y+\frac{z}{3}\right)-(x+y+z)\end{aligned}$$

$$= 15x + 9y + z - x - y - z$$
$$= 14x + 8y.$$

也就是

$$7x + 4y = 100.$$

我们要解“百鸡问题”，就是要寻求 $7x + 4y = 100$ 的非负整数解.

这里的 $7x + 4y = 100$，是一个二元一次不定方程.二元一次不定方程的一般形式是

$$ax + by = c, \tag{3}$$

其中 a、b、c 都是整数.

定理 设二元一次不定方程

$$ax + by = c \tag{3}$$

(其中 a、b、c 都是正整数，而$(a, b) = 1$)有一组整数解 $x = x_0$、$y = y_0$，则它的一切整数解可以表示成

$$x = x_0 - bt, \qquad y = y_0 + at \tag{4}$$

的形式，其中 $t = 0, \pm 1, \pm 2, \cdots\cdots$.

这一定理的证明，可参看一般初等数论书中有关不定方程的讨论，这里从略.

应用这一定理，很容易得出“百鸡问题”的解答. 首先，易见 $s = -1$、$t = 2$ 是不定方程

$$7s + 4t = 1$$

的一组整数解；由此得知 $x = -100$、$y = 200$ 是

$$7x + 4y = 100$$

的一组整数解. 于是，$7x + 4y = 100$ 的一切整数解可以表示成为

$$x=-100-4t, \qquad y=200+7t$$

的形式，其中$t=0$，±1，±2，……．在“百鸡问题”中，由于x、y分别代表公鸡、母鸡的个数，所以必有$x\geqslant0$、$y\geqslant0$．由$-100-4t\geqslant0$得到$t\leqslant-25$，由$200+7t\geqslant0$得到$t\geqslant-\frac{200}{7}$，因此有

$$-\frac{200}{7}\leqslant t\leqslant-25.$$

由于t是整数，故有$t=-28$，-27，-26，-25．又，小鸡的个数是

$$\begin{aligned}z&=100-x-y\\&=100-(-100-4t)-(200+7t)\\&=-3t.\end{aligned}$$

这样，我们就得到了“百鸡问题”的四组解答：

$$\begin{aligned}&x_1=12, \quad y_1=4, \quad z_1=84;\\&x_2=8, \quad y_2=11, \quad z_2=81;\\&x_3=4, \quad y_3=18, \quad z_3=78;\\&x_4=0, \quad y_4=25, \quad z_4=75.\end{aligned}$$

下面再来介绍人们很早就认识了的另一个不定方程：

$$x^2+y^2=z^2, \tag{5}$$

其中x、y、z为正整数．上述不定方程，即是通常所谓的求勾股数组的问题．据史料记载，最简单的一组解$3^2+4^2=5^2$至迟在四千多年前就已被发现．古希腊的毕达哥拉斯（Pythagoras）发现了上述不定方程的部分解的公式：设m是奇数，

$$x=m, \quad y=\frac{m^2-1}{2}, \quad z=\frac{m^2+1}{2}. \tag{6}$$

丢番图也证明了一个部分解的公式：设 m 和 n 是正整数，而 $2mn$ 是一个完全平方数，则

$$\begin{aligned} x &= m+\sqrt{2mn}, \\ y &= n+\sqrt{2mn}, \\ z &= m+n+\sqrt{2mn}. \end{aligned} \tag{7}$$

现今所用的通解公式则是：设 m 和 n 是正整数，$m>n$，$(m, n)=1$，$2\nmid(m+n)$，则方程(5)的满足条件$(x, y)=1$、$2|x$ 的一切正整数解可表示成：

$$\begin{aligned} x &= 2ab, \\ y &= a^2-b^2, \\ z &= a^2+b^2. \end{aligned} \tag{8}$$

通常认为，上式是由罗士琳(公元1789～1853年)得到的，故被称作罗士琳公式.

上面通过"百鸡问题"，介绍了二元一次不定方程的一种一般解法；又介绍了一个二次不定方程——求勾股数组的解，值得注意的是有不少不定方程，解题的特殊性很强，对一个方程适用的方法往往不再适用于另一个方程，要像二元一次方程那样寻求一种"一般解法"实在是很困难的．迄今为止，关于不定方程尚有许多未知领域，真是向人类智慧的挑战.

谈到不定方程，很值得一提的是方程（5）的推广：$x^3+y^3=z^3$，$x^4+y^4=z^4$，……，一般地，$x^n+y^n=z^n$．法国业余数学家费马于 1637 年提出了一则猜想(通常称为"费马大定理")：当 n 是一个大于 2 的整数时，不定方程

$$x^n + y^n = z^n \tag{9}$$

没有正整数解．费马的这一猜想迄今还未被人们证明．1976 年时瓦格斯塔夫(S. Wagstaff)借助于大型电子计算机证得 $2<n<125000$（当然还包括这些数的任何整倍数）情况下这一猜想是成立的．1983 年，联邦德国数学家法尔丁斯(G. Faltings)在《数学创造》杂志上(Invent. Math.)发表了题为《数域上阿贝尔簇的有限性》一文．在此文章中，他以代数几何为主要工具，证明了莫台尔(L. J. Mordell)1922 年提出的一个猜想：数域上任一个亏格 $\geqslant 2$ 的非奇异射影曲线仅有有限多个点的坐标在此数域中．注意到 $n\geqslant 3$ 时，方程(9)定义的曲线满足莫台尔猜想的条件．于是，由莫台尔猜想，立即推出方程(9)对每个 $n\geqslant 3$ 最多只有有限组正整数解．但是，法尔丁斯的方法并未给出(9)中解的个数或上界估计．因而费马大定理仍然未能解决．法尔丁斯这一工作荣获 1986 年度国际数学家大会颁发的菲尔兹奖．

4．同　余

如果 a 与 b 都是整数，而 m 是一个正整数；$(a-b)$ 可以被 m 整除，即 $m|(a-b)$ 时，我们称“a、b 对模 m 同余”，记作 $a\equiv b(\mathrm{mod}\, m)$；当 $m\nmid(a-b)$ 时，称“a、b 对模 m 不同余”，记作 $a\not\equiv b(\mathrm{mod}\, m)$．

显然，我们有

$a\equiv a\ (\mathrm{mod}\ m)$；

若 $a\equiv b(\mathrm{mod}\, m)$，则 $b\equiv a(\mathrm{mod}\, m)$；

若 $a\equiv b(\mathrm{mod} m)$和 $b\equiv c(\mathrm{mod}\, m)$，则 $a\equiv c(\mathrm{mod}\, m)$.

关于同余，还有下列结果：若

$$a_1\equiv b_1(\mathrm{mod}\, m),$$

$$a_2\equiv b_2(\mathrm{mod}\, m),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$a_n\equiv b_n(\mathrm{mod}\, m),$$

则有

$$a_1\pm a_2\pm\cdots\pm a_n\equiv b_1\pm b_2\pm\cdots\pm b_n(\mathrm{mod}\, m), \qquad (10)$$

$$a_1a_2\cdots a_n\equiv b_1b_2\cdots b_n(\mathrm{mod}\, m) \qquad (11)$$

例如，由(11)式和 $10\equiv 1(\mathrm{mod}\ 9)$，我们有 $10^n\equiv 1^n$ $(\mathrm{mod}\ 9)$，即

$$10^n\equiv 1(\mathrm{mod}\ 9). \qquad (12)$$

又，设正整数

$$a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0$$

(其中 $0\leqslant a_i\leqslant 9$，$1\leqslant a_n\leqslant 9$；$i=0,1,2,\cdots,n-1$)，则由(10)、(11)和(12)式，有

$$a\equiv a_n+a_{n-1}+\cdots+a_0\ (\mathrm{mod}\ 9). \qquad (13)$$

根据(13)式，我们可以很快地判别一个整数能否被 9 整除：即只需将这个整数的各位数上的数字加起来，看其数字和能否被 9 整除. 例如 221145236415，它的各数位上的数字之和为

$$2+2+1+1+4+5+2+3+6+4+1+5=36,$$

36 是能被 9 整除的，故 221145236415 亦能被 9 整除.

我们把

$$ax+b\equiv 0\ (\mathrm{mod}\, m) \qquad (14)$$

称为“模 m 的**一次同余式**”，其中 a、b 是整数，且 $a\not\equiv 0$ $(\bmod m)$.

显然，如果整数 c 使 (14) 式成立，即 $ac+b\equiv 0$ $(\bmod m)$，则满足 $x\equiv c\ (\bmod m)$ 的一切整数 x 都能使(14)式成立．于是，我们称

$$x\equiv c\ (\bmod m)$$

为(14)式的一个解．这就是说，把适合(14)式的对模 m 相互同余的一切整数，称为(14)式的一个解.

当$(a,m)\nmid b$ 时，一次同余式 $ax+b\equiv 0(\bmod m)$(其中 $a\not\equiv 0(\bmod m)$) 没有整数解．这可以用反证法来加证明：若存在一个整数 c，使 $ac+b\equiv 0(\bmod m)$，从而有

$$ac-mn=-b,$$

其中 n 为一个整数；又设$(a,m)=l$，则 $a=ld$、$m=le$ (其中 d 和 e 都是整数)；代入上式，有

$$-b=ac-mn=cld-len=l(cd-en),$$

从而 $l|b$，这与已知$(a,m)\nmid b$ 矛盾.

我国古代的《孙子算经》(约公元 400 年)提出了一个问题：

“今有物不知数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

对于这个题，设 x 是所求的“物”的数目，就可以把这个问题归结为求解下列同余式组

$$x\equiv 2(\bmod 3),\quad x\equiv 3(\bmod 5),\quad x\equiv 2(\bmod 7). \tag{15}$$

关于求解一般同余式组

$$x\equiv a(\bmod 3),\quad x\equiv b(\bmod 5),\quad x\equiv c(\bmod 7), \tag{16}$$

有

$$x\equiv 70a+21b+15c\ (\mathrm{mod}\ 105). \qquad (17)$$

这个一般的解法，在我国明朝程大位《算法统宗》(1593年)里，有一首歌：

三人同行七十稀，

五树梅花廿一枝，

七子团圆整半月，

除百零五便得知.

可见关于解同余式组的问题，在我国古代有极光辉的研究成果.

我国古代数学家孙子发明了下面中外驰名的“**孙子定理**”：若 $k\geqslant 2$，而 $m_1, m_2, \cdots, m_k$ 是两两互素的 k 个正整数. 又令

$$M=m_1m_2\cdots m_k=m_1M_1=m_2M_2=\cdots=m_kM_k,$$

则同时满足同余式组

$$x\equiv b_1(\mathrm{mod}\ m_1),\ x\equiv b_2(\mathrm{mod}\ m_2),\cdots,\ x\equiv b_k(\mathrm{mod}\ m_k) \qquad (18)$$

的正整数解是

$$x\equiv b_1M_1'M_1+b_2M_2'M_2+\cdots+b_kM_k'M_k(\mathrm{mod}\ M), \qquad (19)$$

这里 M_i' 是满足同余式 $M_i'M_i\equiv 1(\mathrm{mod}\ m_i)$的正整数解，$i=1, 2, \cdots, k$.

证明 由于当 $i\neq j$ (其中 i、$j=1, 2, \cdots, k$)时$(m_i, m_j)=1$，故$(M_i, m_i)=1$，即

$$(M_1, m_1)=(M_2, m_2)=\cdots=(M_k, m_k)=1.$$

于是，存在整数 M_i' 和 n_i (其中 $i=1, 2, \cdots, k$)，使

$$M_iM_i'+m_in_i=1,$$

即

$$M_iM_i' \equiv 1 \pmod{m_i}.$$

又，当 $i \neq j$ 时，由 $(m_i, m_j) = 1$ 和 $M_j = \frac{M}{m_j}$，可知 $m_i | M_j$. 故有

$$b_jM_j'M_j \equiv 0 \pmod{m_i},$$

从而有

$$b_1M_1'M_1 + b_2M_2'M_2 + \cdots + b_kM_k'M_k \equiv b_iM_i'M_i \equiv b_i \pmod{m_i}.$$

而 $m_1, m_2, \cdots, m_k$ 两两互素，于是

$$x \equiv b_1M_1'M_1 + b_2M_2'M_2 + \cdots + b_kM_k'M_k \pmod{M}$$

是满足(18)式的正整数解.

又，若 y 也能同时满足(18)式，则有

$$x \equiv y \pmod{m_1}, \quad x \equiv y \pmod{m_2}, \quad \cdots, \quad x \equiv y \pmod{m_k},$$

即 $m_1|(x-y), m_2|(x-y), \cdots, m_k|(x-y)$，所以有 $M|(x-y)$，所以

$$x \equiv y \pmod{M}.$$

因此

$$x \equiv b_1M_1'M_1 + b_2M_2'M_2 + \cdots + b_kM_k'M_k \pmod{M}$$

是(18)式的唯一解.

利用孙子定理，即可得到方程(15)的解. 这里，$m_1 = 3$，$m_2 = 5$，$m_3 = 7$；$b_1 = a$，$b_2 = b$，$b_3 = c$. 于是，$M = 105$，$M_1 = 35$，$M_2 = 21$，$M_3 = 15$. 又，设 M_1' 是一个正整数，满足 $M_1'M_1 \equiv 1 \pmod 3$，则有 $1 \equiv M_1'M_1 = 35M_1' \equiv 2M_1' \pmod 3$，得到 $M_1' = 2$. 设 M_2' 是一个正整数，满足 $M_2'M_2 \equiv 1 \pmod 5$，则有 $1 \equiv M_2'M_2 = 21M_2' \equiv M_2' \pmod 5$，得到 M_2'

$=1$.同理,可得 $M_3'=1$.代入(19)式,即可得到(17)式.

我国古代所说的"韩信点兵",就是用孙子定理来解决的一个例子,它是这样一个问题:有兵一列,若列成五行纵队,则末行一人;列成六行纵队,则末行五人;列成七行纵队,则末行四人,列成十一行纵队,则末行十人,求兵数.

对于这个题,设 x 是所求兵数,依题意,有

$$x\equiv 1 \pmod 5,$$
$$x\equiv 5 \pmod 6,$$
$$x\equiv 4 \pmod 7,$$
$$x\equiv 10 \pmod{11}.$$

在孙子定理中,取 $m_1=5$, $m_2=6$, $m_3=7$, $m_4=11$,$b_1=1$, $b_2=5$, $b_3=4$, $b_4=10$,此时,有 $M=5\times6\times7\times11=2310$, $M_1=462$, $M_2=385$, $M_3=330$, $M_4=210$. 又,由 $1\equiv M_1'M_1=462M_1'\equiv 2M_1' \pmod 5$,得 $M_1'=3$;由 $1\equiv M_2'M_2=385M_2'\equiv M_2' \pmod 6$,得 $M_2'=1$;由 $1\equiv M_3'M_3=330M_3'\equiv M_3' \pmod 7$,得 $M_3'=1$;由 $1\equiv M_4'M_4=210M_4'\equiv M_4' \pmod{11}$,得 $M_4'=1$.从而

$$\begin{aligned}x&\equiv 3\times462+5\times385+4\times330+10\times210\\&\equiv 6731\equiv 2111 \pmod{2310}.\end{aligned}$$

即可知

$$x=2111+2310k,\quad 其中\ k=0,1,2,\cdots.$$

我国古代杨辉的《续古摘奇算法》(1275年)和黄宗宪的《求术通解》等数学书中,还有许多类似"韩信点兵"的题目,这说明了我国古代数学家对初等数论作了大量

深入的研究，并取得了光辉的成果.

5. 完全剩余系

设 m 是一个大于1的整数，我们把能被 m 整除的所有整数(即形如 mn 的所有整数，其中 $n=0,\pm1,\pm2,\cdots$)划成一类；把被 m 除后余数是 $m-1$ 的所有整数(即形如 $mn+m-1$ 的所有整数，其中 $n=0,\pm1,\pm2,\cdots$)划成一类；……．这样，我们就把全体整数分成为 m 类．如果从每一类中各取出一个整数，我们把取出的这 m 个整数叫做"模 m 的一个**完全剩余系**"．而把 $0,1,\cdots,m-1$ 称为"模 m 的**非负最小完全剩余系**"．

用 $\varphi(m)$ 表示不大于正整数 m 而和 m 互素的正整数的个数(通常把 $\varphi(m)$ 叫**欧拉**(L. Euler) **函数**)．又设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于 m 而与 m 互素的 $\varphi(m)$ 个正整数．我们把被 m 除后余数是1的所有整数(即形如 $mn+1$ 的所有整数，其中 $n=0,\pm1,\pm2,\cdots$)划为一类；把被 m 除后余数是 a_2 的所有整数（即形如 $mn+a_2$ 的所有整数，其中 $n=0,\pm1,\pm2,\cdots$)划为一类；…；把被 m 除后余数是 $a_{\varphi(m)}$ 的所有整数（即形如 $mn+a_{\varphi(m)}$ 的所有整数，其中 $n=0,\pm1,\pm2,\cdots$)划成一类．这样，我们把所有与 m 互素的整数分成 $\varphi(m)$ 类．从每一类中，各取出一个整数，则这 $\varphi(m)$个整数叫做"以 m 为模的**一个简化剩余系**"．

关于完全剩余系，有一个经过简单推导即可得到的

结果：设 m 是一个大于 1 的整数，而 b、c 是两个任意的整数，但满足条件$(b, m)=1$. 如果 $a_1, a_2, \cdots, a_m$ 是模 m 的一个完全剩余系，则

$$ba_1+c, \quad ba_2+c, \cdots, \quad ba_m+c$$

也是模 m 的一个完全剩余系.

模 m 的简化剩余系也有一个相应的结果，这虽没有上述结果完美，但却非常有用：设 m 是一个大于 1 的整数，a 是一个整数，且满足条件$(a, m)=1$. 如果 b_1，b_2，…，$b_{\varphi(m)}$ 是模m 的一个简化剩余系，则 ab_1，ab_2，…，$ab_{\varphi(m)}$ 也是模 m 的一个简化剩余系.

关于欧拉函数 $\varphi(m)$，有一个定理：设 l 是一个正整数，p 是一个素数，则有

$$\varphi(p^l)=p^{l-1}(p-1). \tag{20}$$

证明 由于 p 是一个素数，于是$1,2,\cdots,p-1$ 中的任何一个整数都与 p 互素，故 $\varphi(p)=p-1$；而当 $l=1$时有 $p^{l-1}=1$，所以当 $l=1$ 时定理成立.

现设 $l>1$，不大于 4 而和 4 互素的正整数是 1，3，共有 2 个，即 $\varphi(4)=2$；不大于 8 而与 8 互素的正整数是1,3,5,7，故 $\varphi(8)=4$；不大于 9 而和 9 互素的正整数是1,2,4,5，7，8，故 $\varphi(9)=6$. 而满足条件 $l>1$ 及 $p^l\leqslant 9$ 的 p^l 只有 4，8，9 这三个数，$\varphi(2^2)=\varphi(4)=2=2^{2-1}(2-1)$，$\varphi(2^3)=\varphi(8)=4=2^{3-1}(2-1)$，$\varphi(3^2)=\varphi(9)=6=3^{2-1}(3-1)$. 故当 $l>1$ 而 $p^l\leqslant 9$ 时，定理亦成立.

现设 $l>1$ 而 $p^l\geqslant 10$. 在不大于 p^l 的正整数中，有 p^{l-1} 个整数：

$$p,\quad 2p,\quad 3p,\quad \cdots,\quad p^{l-1}p$$

是 p 的倍数，其余的不大于 p^l 的正整数都是和 p 互素的.故不大于 p^l 而和 p^l 互素的正整数是 p^l-p^{l-1} 个，即

$$\varphi(p^l)=p^l-p^{l-1}=p^{l-1}(p-1).$$

至此，定理已证完.

对于欧拉函数，还有著名的欧拉定理：设 m 是一个大于 1 的整数，a 是一个整数，且满足条件 $(a,\ m)=1$，则有

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m).$$

证明 设 $1<a_2<\cdots<a_{\varphi(m)}$ 是不大于 m 且和 m 互素的全部正整数.令 r_1 是一个整数，且满足条件

$$a\equiv r_1(\mathrm{mod}\ m),\quad 0\leqslant r_1\leqslant m-1.$$

令 r_i 是一个整数($i=2,\cdots,\ \varphi(m)$)且满足条件

$$aa_i\equiv r_i(\mathrm{mod}\ m),\quad 0\leqslant r_i\leqslant m-1.$$

由于 $1,\ a_2,\ \cdots,\ a_{\varphi(m)}$ 是模 m 的一个简化剩余系，且由 $(a,\ m)=1$，可知 $a, aa_2, \cdots, aa_{\varphi(m)}$ 也是模 m 的一个简化剩余系. 从而 $r_1,\ r_2, \cdots,\ r_{\varphi(m)}$ 和 $1, a_2,\ \cdots,\ a_{\varphi(m)}$ 只是在次序上可能不同，所以

$$r_1r_2\cdots r_{\varphi(m)}\equiv a_2\cdots a_{\varphi(m)}(\mathrm{mod}\ m),$$

进而得到

$$\begin{aligned}a^{\varphi(m)}a_2\cdots a_{\varphi(m)}=a(aa_2)\cdots(aa_{\varphi(m)})&\equiv r_1r_2\cdots r_{\varphi(m)}(\mathrm{mod}\ m)\\&\equiv a_2\cdots a_{\varphi(m)}(\mathrm{mod}\ m).\end{aligned}$$

由于 $a_2,\ \cdots,\ a_{\varphi(m)}$ 与 m 互素，可将上式两端的 $a_2\cdots a_{\varphi(m)}$ 同时消去，得

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m).$$

利用 $\varphi(p)=p-1$（其中 p 为素数），在欧拉定理中取 $m=p$，便得到费马小定理：设 p 为素数，又 $p\nmid a$，则有

$$a^{p-1}\equiv 1(\bmod p). \tag{22}$$

6. 连　分　数

我们称分数

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\ddots+\cfrac{1}{a_N}}}}} \tag{23}$$

为**有限连分数**. 当 $N=\infty$ 时，则简称为**连分数**. 由于上述写法所占篇幅大，一般用记号：

$$a_0+\frac{1}{a_1+}\frac{1}{a_2+}\cdots+\frac{1}{a_N}, \quad 或 \quad [a_0,a_1,a_2,\cdots,a_N]$$

来表示.

设 b 为一个不小于 1 的正数，由

$$(\sqrt{b^2+1}+b)\cdot(\sqrt{b^2+1}-b)=1,$$

可知

$$\sqrt{b^2+1}-b=\frac{1}{\sqrt{b^2+1}+b}. \tag{24}$$

反复用(24)式，有

$$\sqrt{b^2+1}=b+\sqrt{b^2+1}-b=b+\frac{1}{\sqrt{b^2+1}+b}$$

$$=b+\frac{1}{2b+\sqrt{b^2+1}-b}$$

$$=b+\frac{1}{2b+}\frac{1}{\sqrt{b^2+1}+b}$$

$$=b+\frac{1}{2b+}\frac{1}{2b+\sqrt{b^2+1}-b}$$

$$=b+\frac{1}{2b+}\frac{1}{2b+}\frac{1}{\sqrt{b^2+1}+b}$$

$$=\cdots=b+\frac{1}{2b+}\frac{1}{2b+}\cdots+\frac{1}{2b+}\cdots$$

$$=[b,\ 2b,\ 2b,\ \cdots,\ 2b,\cdots]. \tag{25}$$

当 $b\geqslant 2$ 时，利用 $(\sqrt{b^2-1}-b+1)(\sqrt{b^2-1}+b-1)=2(b-1)$，可知

$$\sqrt{b^2-1}-b+1=\frac{2(b-1)}{\sqrt{b^2-1}+b-1}.$$

反复利用上式，有

$$\sqrt{b^2-1}=b-1+\sqrt{b^2-1}-b+1$$

$$=b-1+\frac{2(b-1)}{\sqrt{b^2-1}+b-1}$$

$$=b-1+\cfrac{1}{\cfrac{2(b-1)+\sqrt{b^2-1}-b+1}{2(b-1)}}$$

$$=b-1+\frac{1}{1+}\frac{1}{\sqrt{b^2-1}+b-1}$$

$$=b-1+\frac{1}{1+}\frac{1}{2(b-1)+\sqrt{b^2-1}-b+1}$$

$$=b-1+\frac{1}{1+}\frac{1}{2(b-1)+}\frac{2(b-1)}{\sqrt{b^2-1}+b-1}$$

$$=b-1+\frac{1}{1+}\frac{1}{2(b-1)+}\frac{1}{1+}\frac{1}{\sqrt{b^2-1}+b-1}$$

$$=\cdots=b-1+\frac{1}{1+}\frac{1}{2(b-1)+}\frac{1}{1+}\frac{1}{2(b-1)}$$

$$+\frac{1}{1}+\frac{1}{2(b-1)}+\cdots$$

$$=[b-1,\ 1,\ 2(b-1),1,\ 2(b-1),$$

$$1,\ 2(b-1),\cdots]. \tag{26}$$

对于整数 k（这里 $0\leqslant k\leqslant n$），我们把

$$[a_0,\ a_1,\ a_2,\cdots,\ a_k]=\frac{p_k}{q_k}$$

叫做连分数$[a_0,\ a_1,\ a_2,\cdots,\ a_n]$的**第 k 个渐近分数**．式中 p_k、q_k 皆为 $a_0,\ a_1,a_2,\cdots,a_k$ 的多项式．当 $n\geqslant 3$ 时，$[a_0,\ a_1,\ a_2,\cdots,\ a_n]$的各个渐近分数之间有如下关系式：

$$p_0=a_0,\quad q_0=1,\quad p_1=a_1a_0+1,\quad q_1=a_1. \tag{27}$$

而当 $2\leqslant k\leqslant n$ 时，有

$$p_k=a_kp_{k-1}+p_{k-2},\qquad q_k=a_kq_{k-1}+q_{k-2}. \tag{28}$$

且当 $k\geqslant 1$ 时，有

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}. \tag{29}$$

当 $k\geqslant 2$ 时，有

$$p_kq_{k-2}-p_{k-2}q_k=(-1)^ka_k. \tag{30}$$

对于(27)式和(28)式，当 $k=0,1,2$ 时，可由定义直接验证；而当 $k\geqslant 3$ 时，可用归纳法来证明：即设$m<n$，且

$$[a_0,\cdots,a_m]=\frac{p_m}{q_m}=\frac{a_mp_{m-1}+p_{m-2}}{a_mq_{m-1}+q_{m-2}},$$

其中 p_{m-1}，p_{m-2}，q_{m-1}，q_{m-2} 都只与 a_0，$\cdots$，a_{m-1} 有关，则

$$\frac{p_{m+1}}{q_{m+1}}=[a_0,\cdots,\ a_m,\ a_{m+1}]$$

$$=\left[a_0,\cdots,\ a_{m-1},a_m+\frac{1}{a_{m+1}}\right]$$

$$=\frac{\left(a_m+\frac{1}{a_{m+1}}\right)p_{m-1}+p_{m-2}}{\left(a_m+\frac{1}{a_{m+1}}\right)q_{m-1}+q_{m-2}}$$

$$=\frac{a_{m+1}(a_m p_{m-1}+p_{m-2})+p_{m-1}}{a_{m+1}(a_m q_{m-1}+q_{m-2})+q_{m-1}}$$

$$=\frac{a_{m+1}p_m+p_{m-1}}{a_{m+1}q_m+q_{m-1}}.$$

对于(29)式，当 $k=1$ 时显然成立，由(27)和(28)式,用归纳法便有

$$p_k q_{k-1}-p_{k-1}q_k=(a_k p_{k-1}+p_{k-2})q_{k-1}-p_{k-1}(a_k q_{k-1}+q_{k-2})$$
$$=(-1)^{k-1}.$$

对于(30)式,则可由(27)、(28)和(29)式得

$$p_k q_{k-2}-p_{k-2}q_k=(a_k p_{k-1}+p_{k-2})q_{k-2}-p_{k-2}(a_k q_{k-1}+q_{k-2})$$
$$=a_k(p_{k-1}q_{k-2}-p_{k-2}q_{k-1})$$
$$=(-1)^k a_k.$$

由(26)式,我们有

$$\sqrt{b^2-1}=b-1+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cfrac{1}{1+\cfrac{1}{2(b-1)+\cdots}}}}}}.$$

由此,并注意到 $b-1>0$,我们有

$$b-\frac{4b^2-2b-1}{8b^3-4b^2-4b+1}\leqslant\sqrt{b^2-1}\leqslant b-\frac{4b^2-1}{8b^3-4b}. \tag{31}$$

此外,我们还有

$$\frac{4b^2-2b-1}{8b^3-4b^2-4b+1}-\frac{4b^2-1}{8b^3-4b}$$

$$=\frac{32b^5-16b^4-24b^3+8b^2+4b-32b^5}{(8b^3-4b^2-4b+1)(8b^3-4b)}$$

$$+\frac{16b^4+8b^3+16b^3-8b^2-4b+1}{(8b^3-4b^2-4b+1)(8b^3-4b)}$$

$$=\frac{1}{(8b^3-4b^2-4b+1)(8b^3-4b)}\leqslant\frac{1}{35b^6}. \qquad (32)$$

现在我们来看一个利用连分数开平方的具体例子. 在(31)和(32)式中,取 $b=97$,则我们有

$$56\sqrt{3}=\sqrt{9408}=\sqrt{97^2-1}$$

$$=97-\frac{4\times 97^2-1}{8\times 97^3-4\times 97}+\Delta$$

$$=97-\frac{37635}{7300996}+\Delta,$$

其中
$$-4\times 10^{-13}\leqslant\frac{-1}{35\times 97^6}\leqslant\Delta\leqslant 0,$$

因而有

$$\sqrt{3}=\frac{97}{56}-\frac{37635}{56\times 7300996}+\frac{\Delta}{56}$$

$$=1.732+\frac{0.008}{56}-\frac{37635}{56\times 730096}+\frac{\Delta}{56}.$$

又因

$$0.0000508075688\leqslant\frac{0.008}{56}$$

$$-\frac{37635}{56\times 7300996}\leqslant 0.00005080756889,$$

故有 $\sqrt{3}=1.7320508075688\cdots$.

用相仿的办法,我们还能求出

$$\sqrt{2}=1.4142135623\cdots;$$

$$\sqrt{5}=2.2360679774\cdots;$$

$$\sqrt{13}=3.60555127546\cdots;$$
$$\sqrt{7}=2.645751311004\cdots;$$
$$\sqrt{17}=4.1231056256\cdots;$$
$$\sqrt{19}=4.35889894354067\cdots;$$
$$\sqrt{23}=4.7958315233\cdots;$$

等等.还能用这样的办法来求对数的近似值.

为了求无理数 α 的渐近值，我们称分母不大于某正整数 h 的最接近 α 的分数为 α 的**最佳渐近分数**.而$\frac{p_k}{q_k}$正是 α 的最佳渐近分数，我们作 $\pi=[3, 7, 15, 1, 292, 1, 1, \cdots]$的渐近分数，得

$$\frac{3}{1},\frac{22}{7},\frac{333}{106},\frac{355}{113},\frac{103993}{33102},\frac{104348}{33215},\cdots.$$

在公元 500 年间，我国古代数学家祖冲之曾算出 π 的约率为$\frac{22}{7}$，密率为$\frac{355}{113}$，后者比西方的同样结果要早一千多年. 祖冲之的两率恰为最佳渐近分数之列，即分母不超过 7 时，没有比$\frac{22}{7}$更接近 π 的分数；而分母不超过 113 时，也没有比$\frac{355}{113}$更接近 π 的分数了. 这是我国古代数学家对世界作出的又一重大贡献.

7. 素 数 分 布

前已指出，素数有无穷多个. 素数在自然数列中的分布，是很不规则的. 人们至今没有找到，大概也不可能找到一个可用来表示全体素数的有用公式. 研究各种各样的素数分布状况，一直是数论中最重要和最有吸引力

的中心问题之一.最初的研究方法,是通过观察素数表来发现素数分布的性质. 例如,我们从素数表上即可发现:

在 1 到 100 中间有 25 个素数,

在 1 到 1000 中间有 168 个素数,

在 1000 到 2000 中间有 135 个素数,

在 2000 到 3000 中间有 127 个素数,

在 3000 到 4000 中间有 120 个素数,

在 4000 到 5000 中间有 119 个素数,

在 5000 到 10000 中间有 560 个素数.

可以看出,素数的分布越往上越稀少.

1. 如果以 $\pi(x)$ 表示不大于 x 的素数的个数. 例如,$\pi(2)=1$,$\pi(3)=2$,$\pi(100)=25$,$\pi(1000)=168$. 于是,素数有无穷多便用 $\lim\limits_{x\to\infty}\pi(x)=+\infty$ 来表示. 下面列表表示 x 与 $\pi(x)$之间的一些关系:

x	$\pi(x)$	$x/\ln x$	$\pi(x)/x$	$\pi(x)\ln x/x$
1000	168	144.76…	0.168…	1.1605…
2000	303	263.12…	0.151…	1.1515…
5000	669	587.04…	0.133…	1.1396…
10000	1229	1085.73…	0.122…	1.1319…
50000	5133	4621.16…	0.102…	1.1107…
100000	9592	8685.88…	0.095…	1.1043…
500000	41538	38102.89…	0.083…	1.0901…

从表上可以看出:

(1) x 越大,$\pi(x)$与 x 的比值越接近于 0;

(2) x 越大，$\pi(x)$与 $\frac{x}{\ln x}$的比值越接近于 1.

法国数学家勒让德(A. M. Legendre)和德国数学家高斯猜测：

$$\lim_{x\to\infty}\frac{\pi(x)\ln x}{x}=1,$$

此即著名的**素数定理**.它是素数分布理论的中心定理.

对素数定理，首先做出贡献的是俄国数学家契比雪夫(П. Л. Чебышев)，他在 1852 年左右证明了存在两个正常数 c_1、c_2，使不等式

$$\frac{c_1x}{\ln x}\leqslant\pi(x)\leqslant\frac{c_2x}{\ln x}$$

成立，其中 $x\geqslant2$.

在 1896 年，法国数学家阿达玛(J. Hadamard)和比利时数学家德拉瓦莱–普森 (Ch. J. De la Vallee-Poussin) 彼此独立而又几乎同时证明了素数定理. 他们的证明，都使用了高深的复变函数论知识. 于是，能否以尽可能初等的方法来证明素数定理，便成了数学家们一直探讨的重要问题. 1949 年，美国数学家塞尔伯格(A. Selberg)和埃德斯(P. Erdös)给出了素数定理的初等证明；他们的证明中，除了极限、$\ln x$ 和 e^x 的性质之外，没有用到其他的分析知识，只是证明过程十分复杂. 他们的证明，是基于塞尔伯格的著名恒等式：当 $x\geqslant1$ 时，有

$$\theta(x)\ln x+\sum_{p\leqslant x}\theta\left(\frac{x}{p}\right)\ln p=2x\ln x+O(x), \tag{33}$$

其中 $\theta(x)=\sum_{p\leqslant x}\ln p$；这里 $\sum_{p\leqslant x}$ 表示对所有不超过 x 的素数

求和，记号 O 的定义如下：设 $g(x)>0$，$f(x)$为一复值函数，$a\leqslant x\leqslant b$，若存在一个与 x 无关的正常数 M，使得当 $a\leqslant x\leqslant b$ 时有 $|f(x)|\leqslant Mg(x)$，则记为 $f(x)=O(g(x))$，M称为记号 O 所含之常数．于是，某一满足上述条件的函数 $f(x)$，就可用 $O(g(x))$代之．

2．有误差项的素数定理　是指寻求误差 $\pi(x)-lix$ 的最佳估计，其中函数 $lix=\lim\limits_{\eta\to0}\left(\int_0^{1-\eta}+\int_{1+\eta}^{x}\right)\frac{du}{\ln u}$，它比$\frac{x}{\ln x}$更接近于$\pi(x)$．

德·拉·瓦莱·普森于 1900 年首先证明了 $\pi(x)-lix=O(x\exp(-c\sqrt{\ln x}))$，这里$c$是一个正的常数．冯·科奇(von Koch)于1901 年在黎曼假设(参见本书第 46 页)下证明了 $\pi(x)-lix=O(x^{\frac{1}{2}}\ln x)$．维诺格拉道夫(И. М. Виноградов)于 1958 年借助他的三角和估计方法(参见本书第 34 页)，得到 $\pi(x)-lix=O(x\exp(-c(\ln x)^{\frac{3}{5}-\varepsilon}))$，其中 ε 为任意正数，c 是和 ε 有关的正常数．误差项 $\pi(x)-lix$ 的变化是极不规则的．设 $f(x)$是实函数，如果存在与 x 无关的正常数 a，使得某些任意大的 x 满足$f(x)>ax$，则记为 $f(x)=\Omega_+(x)$；若使得某些任意大的 x 满足$f(x)<-ax$，则记为 $f(x)=\Omega_-(x)$．若这两种情形同时出现，则记为 $f(x)=\Omega_\pm(x)$．英国数学家李特伍德(J. E. Littlewood)于 1914 年证明了：当 $x\to\infty$ 时，有 $\pi(x)-lix=\Omega_\pm((x^{\frac{1}{2}}\ln\ln\ln x)/\ln x)$．

3．算术级数中的素数定理　狄利克雷于 1837 年首

先证明了首项与公差互素的算术级数中有无限多个素数. 设整数 $q \geqslant 3$, $1 \leqslant l \leqslant q$, $(l, q)=1$. 以 $\pi(x, q, l)$ 表首项为 l 公差为 q 的算术级数中不超过 x 的素数之个数. 类似于素数定理,对于固定的 q,容易证明:

$$\lim_{x \to \infty} \frac{\pi(x,q,l)\varphi(q)\ln x}{x} = 1,$$

其中 $\varphi(q)$ 表示不超过 q 且与 q 互素的正整数的个数. 这就是通常所说的"算术级数中的素数定理".

关于误差项估计,帕吉(A. Page)于 1935 年,西格尔(C. L. Siegel)与瓦尔菲什(A. Walfisz)于 1936 年,先后证明了:对任意正数 h,当 $3 \leqslant q \leqslant (\ln x)^h$ 时,有 $\pi(x,q,l) - \frac{1}{\varphi(q)} li x = O(x\exp(-c\sqrt{\ln x}))$, 其中 c 为绝对正常数,记号 O 中所含的常数仅与 h 有关,而与 q 无关.

4. 算术级数中的最小素数　设 $k \geqslant 3$, $1 \leqslant l \leqslant k$, $(l,k)=1$,以 $p(k, l)$表示算术级数 $kn+l$(其中 $n=0,1,2,\cdots$)中的最小素数. 乔拉(s. chowla)猜测 $p(k, l)=O(k^{1+\varepsilon})$,其中 ε 为任意小的正数. 林尼克(Ю. Б. Линник)于1944年首先证明了存在绝对常数 c,使得 $p(k, l)=O(k^c)$. 潘承洞于 1957 年首先指出 c 是可以计算的,并定出了 c 的值. 目前最好的结果是 $c \leqslant 15$,这是我在 1979 年得到的.

5. 孪生素数猜想　两个差等于 2 的一对素数,叫做**孪生素数**. 例如,3 和 5; 5 和 7; 11 和 13; 17 和 19; 29 和 31; 41 和 43; 59 和 61; 71 和 73; 101 和103; …; 10016957

和 10016959，都是孪生素数．迄今所知的最大孪生素数是 $1159142985\times2^{2304}-1$，$1159142985\times2^{2304}+1$；它们是阿特金(A. O. L. Atkin)和赖克特 (N. W. Rickert)于 1979 年得到的．所谓“孪生素数猜想”，是指猜测：存在无穷多对孪生素数．这个猜想至今没有解决；但是，认为它是正确的可能性很大．在这方面，最好结果是我在 1966 年得到的：存在无穷多个素数 p，使得 $p+2$ 是不超过两个素数之积．

6．相邻素数之差　设 p_n 是第 n 个素数，$d_n=p_{n+1}-p_n$ 是相邻的两个素数之差．在黎曼假设下，克拉梅 (H. Cramér)于 1921 年证明了 $d_n=O(p_n^{\frac{1}{2}}\ln p_n)$．无条件结果 $d_n=O(p_n^{\frac{11}{20}+\varepsilon})$是赫斯–布劳恩(D.R. Heath–R. Brown)和伊瓦尼斯(H. Iwaniec)于 1979 年得到的．另一方面，关于 d_n 的下界，博姆比里(E. Bombieri) 和达温波特 (H. Davenport)于 1966 年证明了：

$$E=\lim_{n\to\infty}\inf\frac{d_n}{\ln p_n}\leqslant\frac{2+\sqrt{3}}{8}=0.46650\cdots.$$

休克斯勒伊(M.N.Huxley)于1977年改进为 $E\leqslant0.4425$，猜测应有 $E=0$．关于 d_n，还有许多有趣的研究．

8．关于完全数和麦森素数

在欧几里得时代，还研究过的一个数论问题是完全数．

对于一个自然数 n，如果它的所有正因数之和恰等于 $2n$，那么这个数便叫做**完全数**.

例如数 6，它的所有正因数是 1,2,3,6；由于 $1+2+3+6=12=2\times6$，所以 6 是完全数.

最小的五个完全数是 6,28,496,8128,33550326.

欧几里得在《原本》里证明了一个定理：如果 p 为素数，且 2^p-1 也为素数，那么 $2^{p-1}(2^p-1)$ 就是一个偶的完全数.

欧拉证明了上述定理的逆定理仍成立.

欧几里得与欧拉的结果只给出了偶完全数形状的一个充分必要的条件.那么，是否存在奇完全数呢？至今，人们还从未发现有这样的数存在，并且倾向于猜想不存在奇完全数.但是，这个问题至今没有解决. 除了欧拉曾对奇完全数的形状给出过一个必要条件外，迄今我们所知关于这一问题发表的结果，主要是给出奇完全数的下界估计.目前，我们所知的结果是：如果奇完全数存在，则它必定大于 10^{200}，且有至少八个不同的奇素因子.

即使对偶完全数，同样提出了：偶完全数只有有限多个，还是有无穷多个？迄今，我们仅发现了 28 个偶完全数.

和偶完全数相对应的，是麦森(**M. Mersenne**)素数.设 p 是素数，我们把形如 2^p-1 的素数叫做**麦森素数**，记作

$$M_p=2^p-1.$$

根据上述欧几里得的定理，可知有一个麦森素数，便

可构造出一个偶完全数.

目前我们所知道的最大的麦森素数是 M_{216091}，它有65050位数字，是1985年发现的. 在证明它为素数时，需要用特殊的方法，并借助于电子计算机.

二、解析数论

解析数论是用数学分析的工具来解决数论问题. 它的基础是由瑞士数学家欧拉建立的，然后，经狄利克雷、黎曼(G. F. B. Riemann)、维诺格拉道夫、华罗庚等数学家的工作，将它发展起来了. 数论中的这一个分支，与复变函数紧密地联系着. 由于在不连续的整数之间，经过引入连续量，而导出了新的联系，因此解析方法使数论的内容变得更充实. 这就使近一个多世纪以来解析数论成为数论中最有生气的一个分支. 我国著名数学家华罗庚教授早在三十年代，就从事对许多著名解析数论问题的研究，并取得了许多重大的成果. 五十年代以后，他在中国科学院数学研究所带领一批青年数学工作者，继续从事这方面的研究. 另外，闵嗣鹤教授也在北京大学数学力学系开设了解析数论专业课程. 在他们的热情指导和悉心培养下，我国年青的数学工作者对解析数论中许多著名问题做了大量的研究工作，并取得了好些在世界上占领先地位的硕果. 可以认为，解析数论是迄今为止我国在近代数学中取得重大进展的最突出的数学分支之一. 由于普

及解析数论知识有一定难度，这里只能简要介绍解析数论中的一些著名难题，并结合谈谈解析数论中的一些基本方法．

1．三 角 和

在素数分布问题上，前面曾谈到算术级数中的最小素数问题．这问题目前的最好的结果，是一部分借助于维诺格拉道夫的三角和估值方法得到的．下面简单介绍这个方法．形如

$$\sum_{A<x<B} e^{2\pi i f(x)} \tag{34}$$

的和数，称为**三角和**，其中 $f(x)$ 是 x 的一个实值函数，而 x 经过 A 到 B 之间的所有整数，或经过 A 到 B 的某些整数（例如，经过 A 到 B 的全部素数）．

当 $f(x)$ 为整数时，由于 $e^{2\pi i f(x)}$ 的模为 1，因而

$$\left|\sum_{x=1}^{p} e^{2\pi i f(x)}\right| \leqslant p. \tag{35}$$

关于这个估计，由于 $f(x)$ 不一定都是整数，因而在许多情况下可以得到本质上的改进．令 $f(x)$ 是多项式

$$f(x)=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\cdots+\alpha_1 x+\alpha_0.$$

若所有的 α_i（其中 $i=0,1,\cdots,n$）都是整数，则当 x 为整数时，(35)式的估计不能改进．但若 α_i 不全是整数时，维诺格拉道夫利用有理分数来接近这些素数的方法，可以得到更精确的估计．

三角和方法的出现，使数论中一些著名问题得到了

解决，其中最有名的是维诺格拉道夫在 1937 年基本解决的三素数问题，即哥德巴赫猜想中的两个问题之一.

1742 年，德国数学家哥德巴赫在与欧拉通信时，提出了关于正整数与素数之间的堆垒性质的两个猜测：

(A) 每一个不小于 6 的偶数，皆可表为两个奇素数之和；

(B) 每一个不小于 9 的奇数，皆可表为三个奇素数之和.

这就是著名的数论难题——**哥德巴赫猜想**.

由于 $2n+1=2(n-1)+3$，因而，从猜想(A)的正确性，可立即推出猜想(B)的正确性.

欧拉对这个猜想的正确性是深信不疑的，他说："尽管我还不能证明出来，但我认为这是一个肯定的定理."可是，哥德巴赫猜想已提出了二百多年，至今还不能最后肯定其正确性. 维诺格拉道夫证明了：充分大的奇数，皆可表为三个奇素数之和，从而基本上解决了猜想 (B). 1966年，我利用所提出的新的加权筛法，证明了：每一个充分大的偶数，都可以表为一个素数与一个不超过两个素数的乘积之和. 这是至今对猜想(A)的最好结果. 由于猜想(B) 基本上解决了，因而，现在讲到哥德巴赫猜想时，总是指猜想(A).

2. 古 典 筛 法

如果 $\mathscr{A}$ 是一个满足一定条件的由有限多个整数组

成的集合，其中元素可以重复．而 $\mathscr{P}$ 表示一个满足一定条件的无限多个不同的素数组成的集合。设正数 $z\geqslant 2$，又令

$$P(z)=\prod_{\substack{p<z\\ p\in\mathscr{P}}} p.$$

用 $S(\mathscr{A};\mathscr{P};z)$ 表示集合 $\mathscr{A}$ 中所有和 $p(z)$ 互素的元素的个数，即

$$S(\mathscr{A};\mathscr{P},z)=\sum_{\substack{a\in\mathscr{A}\\ (a,p(z))=1}} 1.$$

于是，$p(z)$好像是一个"筛子"，凡是和它不互素的数都被"筛掉"了，而和它互素的数就被留下．可以看出，"筛子"$p(z)$与集合 $\mathscr{P}$ 及 z 有关：z 越大，则"筛子"越大，而被"筛掉"的数就越多．$S(\mathscr{A};\mathscr{P},z)$就是指集合 $\mathscr{A}$ 经过 $p(z)$"筛选"后所剩下的元素个数．称 $S(\mathscr{A};\mathscr{P},z)$为**筛函数**．所谓筛法，即是研究筛函数的性质与作用的方法．由于 $S(\mathscr{A};\mathscr{P},z)$总是非负整数，于是，一个基本问题就是去估计筛函数 $S(\mathscr{A};\mathscr{P},z)$的上界和下界．

利用筛法，我们设想一个解决哥德巴赫猜想的方法，即能否先证明每一个充分大的偶数是两个素因子不多的乘积之和，然后再想法逐步减少素因子的个数．为此，我们设 a、b 为两个正整数，以$\{a,b\}$表示命题：每一个充分大的偶数，是一个不超过 a 个素数的乘积与一个不超过 b 个素数的乘积之和．这样，哥德巴赫猜想即是去证明命题$\{1,1\}$．为了把命题$\{a,b\}$与筛函数联系起来，我们设 N 为一大偶数，令集合

$$\mathscr{A}=\mathscr{A}(N)=\{n(N-n);1\leqslant n\leqslant N\},$$

$\mathscr{P}$ 为所有素数组成的集合.又设 $\lambda\geqslant 2$,取 $z=N^{\frac{1}{\lambda}}$. 若能证明

$$S(\mathscr{A};\ \mathscr{P},\ N^{\frac{1}{\lambda}})>0, \tag{36}$$

则显然证明了命题$\{a,\ a\}$,其中

$$a=\begin{cases}\lambda-1, & \text{当 } \lambda \text{ 是正整数时;}\\ [\lambda], & \text{当 } \lambda \text{ 不是正整数时.}\end{cases}$$

若当 $\lambda=2$ 时,(36)式成立,则证明了命题$\{1,1\}$. 又若求出了 $S(\mathscr{A};\ \mathscr{P},\ N^{1/\lambda})$的一个上界,则相应地得到了一个大偶数表为二个素因子不超过 a 个的数之和的表示方法的个数之上界.

若取集合

$$\mathscr{B}=\mathscr{B}(N)=\{N-p;\ p<N\},$$

则如果能证明

$$S(\mathscr{B};\ \mathscr{P},\ N^{\frac{1}{\lambda}})>0,$$

就证明了命题$\{1,\ a\}$.相应地,若求出 $S(\mathscr{B};\ \mathscr{P},\ N^{\frac{1}{\lambda}})$的一个上界,则得到了一个大偶数表为一个素数与一个素因子不超过 a 个的数之和的表法个数的上界.

由以上的讨论知道,命题$\{a,a\}$和求筛函数的正的下界与上界这一问题是相关联的. 但是,应该说明,这里要求 z 所取的值对于 N 来讲不能太小,必须取 $N^{\frac{1}{\lambda}}$ 那么大的阶. 当然,我们希望 λ 能取得越小越好,即 z 能尽可能取得大一些,古典筛法理论中,仅能对较小的 z(例如,取 z 为 $\log_c N$)时才能证明筛函数有正的下界,但这对哥德巴赫猜想来讲是无用的. 挪威数学家布龙(V.Brun)首先

对古典筛法作了改进,他在1920年左右因此而证明了命题{9,9}. 从此,许多数学家便利用筛法来解决哥德巴赫猜想. 但布龙筛法有很强的组合数学的特征,比较复杂. 在其思想的启发下,1950年左右,塞尔伯克利用求二次型极值的方法对筛法作了另一重大改进,从而可得到筛函数的下界估计. 另外,在1941年库琴首先提出了"加权筛法",这使我们能在同样的筛函数的上、下界估计中得到更强的结果. 然而,上述的方法都有一个共同的弱点,即还不能证明命题{1, b}. 1941年左右,林尼克发明了"大筛法",因而在1948年匈牙利数学家雷奈(A. Rényi)利用大筛法研究L函数的零点分布,进而再利用布龙筛法,证明了{1, b},但未定出b的值. 以后,由我国数学家王元、潘承洞等及国外许多数学家对其结果进行改进,而分别证明了命题{1,5},{1,4}和{1,3}.

3. 大 筛 法

设$\mathscr{A}$是一个由有限多个整数所组成的集合,$X>2$,$\mathscr{P}$是一个由有限个不同的素数p所组成的集合($p\leqslant x$). 再设对每一个素数$p\in\mathscr{P}$,给定模p的$\lambda(p)$个不同的剩余类:

$$h_{p,1},\quad h_{p,2},\quad \cdots,\quad h_{p,\lambda(p)}.$$

在集合$\mathscr{A}$中,筛去所有满足下述条件的元素n:

$$n\equiv h_{p,j}(\bmod p),\quad 1\leqslant j\leqslant\lambda(p),\quad p\in\mathscr{P},$$

把这样筛剩下来的$\mathscr{A}$的子集合记为N,并设其元素个

数为 Z.筛法所研究的主要问题，就是去估计 Z 的上界和下界．按照所有的 $\lambda(p)$ 是“大”还是“小”，就称相应的筛法为“大筛法”和“小筛法”．例如，取 $\lambda(p)=1$，$h_{p,1}=0$，这就是通常称为“小筛法”的筛法．林尼克首先考虑了这样的问题：设集合 $\mathscr{A}$ 是由整数 $M+1, M+2, \cdots, M+N$ 这样 N 个相邻的整数组成，取 $X=N^{\frac{1}{2}}$，而 $\mathscr{P}$ 由

$$2 \leqslant p_1 < p_2 < \cdots < p_y \leqslant N^{\frac{1}{2}}$$

这 y 个不同的素数组成．设

$$\lambda = \min_{1 \leqslant i \leqslant y} \frac{\lambda(p_i)}{p_i}, \quad \text{且满足 } 0<\lambda<1.$$

则对 Z 有估计：

$$Z \ll \frac{N}{\lambda^2 y},$$

其中符号“$\ll$”表示可计算的绝对常数．

由于 $\lambda(p_i) \geqslant \lambda p_i$，所以是“大”的，从而叫做“大筛法”．雷奈进一步精确化，他考虑和式

$$\sum_{p \in \mathscr{P}} pD(p), \tag{37}$$

其中

$$D(p) = \sum_{h=0}^{p-1} \left| Z(p, h) - \frac{Z}{p} \right|^2,$$

$$Z(p, h) = \sum_{\substack{n=m+1 \\ n \equiv h (p)}}^{m+N} a_n,$$

而

$$a_n = \begin{cases} 1, & \text{当 } n = n_i, 1 \leqslant i \leqslant Z \text{ 时；} \\ 0, & \text{其他．} \end{cases}$$

则(37)式是刻划 $n_1, n_2, \cdots, n_z$ 这 z 个整数在所有模 $p(p$

$\in \mathscr{P}$)的所有剩余类中分布状况的一种度量.雷奈先用林尼克的方法证明了:当

$$X = N^{\frac{1}{3}} Z^{-\frac{1}{6}} |\mathscr{P}|^{\frac{1}{6}}$$

时,有

$$\sum_{p \in \mathscr{P}} pD(p) \ll Z^{\frac{2}{3}} N^{\frac{4}{3}} |\mathscr{P}|^{\frac{1}{3}}.$$

进而,他改进其结果,证明了:若取 $\mathscr{P}$ 为所有 $p \leqslant X$,则当 $X \leqslant N^{\frac{4}{5}} Z^{-\frac{1}{5}}$ 时,有

$$\sum_{p \leqslant X} pD(p) \ll Z(N + X^3).$$

特别,取 $X = N^{\frac{1}{3}}$ 时,有

$$\sum_{p \leqslant N^{\frac{1}{3}}} pD(p) \ll ZN.$$

于是,大筛法归结为对(37)式的上界估计. 1965 年,罗思及博比里分别证明了

$$\sum_{p \leqslant N^{\frac{1}{2}} (\log N)^{-\frac{1}{2}}} pD(p) \ll ZN$$

和

$$\sum_{p \leqslant N^{\frac{1}{2}}} pD(p) \ll ZN.$$

利用大筛法,还可以得到算术级数中素数分布的一类新的均值估计:

令 $\mathscr{E}_x$ 是一个与参数 x 有关的集合,设

$$g(a) = g_x(a) = \sum_{\substack{e \in \mathscr{E}_x \\ e = a}} 1.$$

并假定存在一个正值函数$E(x)$,使对所有正整数 $e \in \mathscr{E}_x$,均有 $e \leqslant E(x)$成立.若对算术级数

$n = l + kd$, 其中 $k = 0, \pm 1, \pm 2, \cdots$, $(l, d) = 1, d \geqslant 1$,

存在正数 α(这里 $0<\alpha\leqslant 1$),使 $\frac{1}{2}\leqslant E(x)\ll x^{1-\alpha}$; 且存在一正整数 r (与 x 无关),使 $g_x(a)\ll d^r(a)$, 其中 $d(a)$为除数函数,则对任给正数 A,当

$$B=\frac{3}{2}A+2^{2r+2}+13$$

时,有

$$\bar{R}(D, x, \mathscr{E}_x)=\sum_{d<D}\max_{y<x}\max_{(l,d)=1}\left|\sum_{\substack{a<E(x)\\(a,d)=1}}g_x(a)\left(\sum_{\substack{an<y\\an\equiv l(d)}}\Lambda(n)-\frac{1}{\varphi(d)}\sum_{an<y}\Lambda(n)\right)\right|\ll\frac{x}{\log^A x}$$

和

$$R(D, x, \mathscr{E}_x)=\sum_{d\leqslant D}\max_{y<x}\max_{(l,d)=1}\left|\sum_{\substack{a\leqslant E(x)\\(a,d)=1}}g_x(a)\left(\sum_{\substack{an\leqslant y\\an\equiv l(d)}}\Lambda(n)-\frac{1}{\varphi(d)}\frac{y}{a}\right)\right|\ll\frac{x}{\log^A x}\qquad(38)$$

成立,其中 $D=x^{\frac{1}{2}}\log^{-B}x$.

这类新的均值定理,对命题{1,2}的证明,起了关键性的作用.

4. 大筛法在证明哥德巴赫猜想中的应用

设 b 为一正整数,N 为一大偶数,集合

$$\mathscr{A}^{[b]}=\mathscr{A}^{[b]}[N]=\{a;\ a\in\mathscr{A},\ v_2(a)\leqslant b\},$$

其中 $v_2(a)$表示 a 的全部素因子个数(按重数计). 这样,$\mathscr{A}^{[b]}$是集合 $\mathscr{A}$ 中所有素因子个数不超过 b 个的元素所组成的子集. 这样,命题{1, b}就是要证明,对充分大的

偶数 N，必有

$$|\mathscr{A}^{[b]}|>0.$$

设 $v_1(N)$ 为 N 的不同素数因子的个数．由于 $a\in\mathscr{A}$，$(a, N)>1$ 的元素个数 $\leqslant v_1(N)\ll\log N$，故

$$\begin{aligned}\mathscr{A}^{[b]}&\geqslant\sum_{\substack{a\in\mathscr{A}\\(a,p(N^{\frac{1}{b+1}}))=1}}1+O(v_1(N))\\&=S(\mathscr{A};\mathscr{P},N^{\frac{1}{b+1}})+O(\log N).\end{aligned}$$

当取 $b=4$ 时，可以得到

$$|\mathscr{A}^{[4]}|\geqslant(1+O(1))8\log^{\frac{3}{2}}c(N)\frac{N}{\log^2 N}>0,$$

从而证明了命题{1，4}成立．

若利用库琴首先提出的加权筛法，可得

$$|\mathscr{A}^{[b]}|\geqslant\sum_{\substack{a\in\mathscr{A}\\(a,P(N^{\frac{1}{v}}))=1}}\left(1-\frac{1}{2}\rho_1(a)\right)+O(N^{1-\frac{1}{v}}),$$

其中，正整数 $v>b\geqslant1$ 而

$$\rho_1(a)=\sum_{\substack{p_1|a,p_1\nmid N\\N^{\frac{1}{v}}<p_1<N^{\frac{1}{b}}}}1,\qquad P(Z)=\prod_{\substack{p<z\\p\nmid N}}p.$$

当取 $b=3$，$v=10$ 时，便有

$$|\mathscr{A}^{[3]}|>2.64\,c(N)\frac{N}{\log^2 N}>0.$$

于是，命题{1，3}得到了证明．

可以看出，在证明命题{1，4}和命题{1，3}时，为了用筛法来估计 $|\mathscr{A}^{[b]}|$ 的下界，前者是直接去估计最简单的筛函数：

$$S(\mathscr{A};\mathscr{P},z)=\sum_{\substack{a\in\mathscr{A}\\(a,p(z))=1}}1;$$

而后者是去估计“加权”的筛函数

$$S(\mathscr{A};\mathscr{P},z,\rho)=\sum_{\substack{a\in\mathscr{A}\\(a,p(z))=1}}\rho(a),$$

即对每一个元素 a，加上一个权函数 $\rho(a)$．在证明命题{1，4}时，可以看成是权函数 $\rho(a)=1$，而证明命题{1，3}时，$\rho(a)=1-\frac{1}{2}\rho_1(a)$．权函数 $\rho(a)$的形式可以多种多样，但是引进新的权函数后，估计的复杂性也会大大增加．

我在证明命题{1，2}时，提出了新的加权筛法．设 b 为正整数，v 为正数，$v>b\geqslant 2$，则有

$$|\mathscr{A}^{[b-1]}|\geqslant\sum_{\substack{a\in\mathscr{A}\\(a,p(N^{\frac{1}{v}}))=1}}\left(1-\frac{1}{2}\rho_1(a)-\frac{1}{2}\rho_2(a)\right)+O(N^{1-\frac{1}{v}}),$$

其中 $\rho_1(a)$与前相同，

$$\rho_2(a)=\begin{cases}1, & a=p_1p_2\cdots p_b,\ N^{\frac{1}{v}}\leqslant p_1<N^{\frac{1}{b}}\leqslant p_2<\cdots\\ & <p_b,\ (a,N)=1;\\ 0, & \text{其他}.\end{cases}$$

在上式中，取 $b=3$、$v=10$，则可得

$$\begin{aligned}|\mathscr{A}^{[2]}|&\geqslant\sum_{\substack{a\in\mathscr{A}\\(a,P(N^{\frac{1}{10}}))=1}}\left(1-\frac{1}{2}\rho_1(a)\right)-\frac{1}{2}\Omega_2+O(N^{\frac{9}{10}})\\&\geqslant 4(1+6\log 3-10\log 2)(1+O(1))c(N)\\&\quad\times\frac{N}{\log^2 N}-\frac{1}{2}\Omega_2+O\left(\frac{N}{\log^3 N}\right),\end{aligned}$$

其中

$$\Omega_2=\sum_{\substack{a\in\mathscr{A},(a,N)=1\\(a,p(N^{\frac{1}{10}}))=1}}\rho_2(a)=\sum_{\substack{N^{\frac{1}{10}}\leqslant p_1<N^{\frac{1}{3}}\leqslant p_2<\left(\frac{N}{p_1}\right)^{\frac{1}{2}}\\(p_1p_2,N)=1}}\ \sum_{\substack{a\in\mathscr{A},a=p_1p_2p_3\\p_2<p_3,p_3\nmid N}}1.$$

这样，为了证明命题{1,2}，只需估计 Ω_2 的上界，由于 $a \in \mathscr{A}$ 时，$a = N - p$，$p < N$，所以对固定的 p_1、p_2，有

$$\sum_{\substack{a \in \mathscr{A},\, a = p_1 p_2 p_3 \\ p_2 < p_3,\, p_3 \nmid N}} 1 = \sum_{\substack{p = N - p_1 p_2 p_3 \\ p_2 < p_3 < \frac{N}{p_1 p_2},\, p_3 \nmid N}} 1,$$

因而

$$\Omega_2 = \sum_{\substack{N^{\frac{1}{10}} \leqslant p_1 < N^{\frac{1}{8}} \leqslant p_2 < \left(\frac{N}{p_1}\right)^{\frac{1}{2}} \\ (p_1 p_2, N) = 1}}' \sum_{\substack{p = N - p_1 p_2 p_3 \\ p_2 < p_3 < \frac{N}{p_1 p_2},\, p_3 \nmid N}} 1.$$

这样，就把原来 Ω_2 是估计元素 a 的个数，转化为估计素数 p 的个数，从而得到

$$\Omega_2 \leqslant S(\mathscr{L}; \mathscr{P}, z) + O(N^{\frac{2}{3}}), \qquad z \leqslant N^{\frac{13}{80}},$$

其中 $\mathscr{L} = \{l;\ l = N - ep,\ e \in \mathscr{E},\ ep \leqslant N\}$，而

$$\mathscr{E} = \left\{e;\ e = p_1 p_2,\ N^{\frac{1}{10}} \leqslant p_1 < N^{\frac{1}{8}} \leqslant p_2 < \left(\frac{N}{p_1}\right)^{\frac{1}{2}},\ (p_1 p_2, N) = 1\right\},$$

又 $\mathscr{P} = \{p;\ p \nmid N\}$.

再应用前面所提到的算术级数中素数分布的一类新的均值估计(38)式（取 $z^2 = D = N^{\frac{1}{2}} \log^{-B} N$，$B_1 = 248$），就有

$$\Omega_2 < 6(2\log 10 - \log 3 - \log 17)(1 + O(1))c(N)\frac{N}{\log^2 N},$$

从而证明了命题{1,2}.

在这里，我们取权函数 $\rho(a) = 1 - \frac{1}{2}\rho_1(a) - \frac{1}{2}\rho_2(a)$，虽然使估计变得更困难，但是最终还是证明了命题{1,2}. 需要指出的是，这种加权筛法不可能用来证明命题{1,1}，因为这时要取 $b = 2$，而这使得主项和余项的估计

中出现至今仍然无法克服的困难.

5. 黎曼ζ函数

黎曼ζ函数,是指复变函数 $\zeta(s)$:

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}, \tag{39}$$

其中 $s=\sigma+it$ 是复数,$\sigma>1$.

实变数情形的黎曼ζ函数,欧拉早就讨论过.他曾利用算术基本定理,证明了:当 $\sigma>1$ 时,有恒等式

$$\zeta(s)=\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1},$$

其中 $\prod_{p}$ 表示对所有的素数求积.

复变数 s 的函数 $\zeta(s)$ 是黎曼于1859年发表的《论不大于一个给定值的素数个数》(Über die Anzahl Primzahlen unter einer gegebenen Grösse) 著名论文中第一次提出的.他严格证明了:

(1) $\zeta(s)$ 可解析开拓到全平面,且满足函数方程

$$\zeta(1-s)=2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\Gamma(s)\zeta(s).$$

(2) 除了 $s=1$ 是一个残数为1的一次极点外,$\zeta(s)$ 在整个平面上是正则的.

(3) 当 $\sigma>1$ 时,$\zeta(s)$没有零点.

(4) 当 $\sigma<0$ 时,$s=-2,-4,\cdots,-2n,\cdots$ 是它的一级零点,这些零点称为 $\zeta(s)$ 的"无聊零点" (trivial zeros).除此之外,$\zeta(s)$没有零点.

(5) 当 $0 \leqslant \sigma < 1$ 时，$\zeta(\sigma) \neq 0$.

(6) $\zeta(s)$可能有的其它零点一定是都位于带形区域 $0 \leqslant \sigma \leqslant 1$ 中的复零点，它们称为“非无聊零点”.

此外，他还给出了一些深刻的结果，而为后来的其他人所证明，例如，

(7) 在带形区域 $0 \leqslant \sigma \leqslant 1$ 中，$\zeta(s)$有无穷多个复零点. 这是 1893 年为法国数学家阿达玛所证明的.

(8) 设 $T > 0$，以 $N(T)$ 表示 $\zeta(s)$ 在矩形 $0 \leqslant \sigma \leqslant 1$，$0 < t < T$ 中的零点个数，则有 $N(T) \sim \frac{T}{2\pi} \ln \frac{T}{2\pi} - \frac{T}{2\pi}$. 这是 1905 年为冯·曼戈德 (H. von Mangoldt) 所证明的.

(9) 建立了 $\zeta(s)$的非无聊零点与 $\pi(x)$(不超过 x的素数个数)之间的一个关系式. 这是 1894 年为冯·曼戈德所证明的. 这一关系式揭示了素数定理与 $\zeta(s)$的非无聊零点的分布有密切关系，指明了研究素数定理的方向.

黎曼还在他的这篇著名论文中提出了一个影响深远的猜测：$\zeta(s)$ 的所有非无聊零点都位于直线 $\operatorname{Re} s = \frac{1}{2}$ 上，即所谓“黎曼假设”，简记作 RH.

1974 年，莱温桑(N. Levinson)证明了：$\zeta(s)$至少有多于 1/3 的零点位于直线 $\operatorname{Re} s = \frac{1}{2}$ 上.

1982年，布伦特(R. P. Brent)等四人证明了：$\zeta(s)$在矩形 $0 \leqslant \sigma \leqslant 1, 0 \leqslant t \leqslant 81702130.19$ 中的零点，全部位于直线 $\operatorname{Re} S = \frac{1}{2}$ 上，共有200000001个零点，都是一级零点.

但是，黎曼假设至今还没有被证明，或被否定．从黎曼假设出发，可以推出一系列重要的数论和函数论方面的结果，虽然都是些假设性的（其中有的在后来被证明），但是这些结果指出了研究 $\zeta(s)$ 零点的重要意义和方向．1896 年阿达玛和德拉瓦莱–普森（Ch. J. De la Vallee-Poussin）各自独立证明了 $\zeta(s)$在直线 $\sigma=1$ 上没有零点，并推出了素数定理．德拉瓦莱–普森又于 1900 年证明了存在一个正常数 A_1，使得 $\zeta(s)$ 在区域 $\sigma\geqslant 1-A_1(\ln(|t|+2))^{-1}$中没有零点，并得到了有误差项的素数定理．苏联数学家维诺格拉道夫于 1958 年证明了存在一个正常数 A_2，使得对任意的 $\varepsilon>0$，$\zeta(s)$在区域 $\sigma\geqslant 1-A_2(\ln(|t|+2))^{-\frac{2}{3}-\varepsilon}$ 中没有零点，其中 A_2 和 ε 有关，并改进了有误差项的素数定理．素数定理的进展，是严格按照黎曼所提出的思想、方法和结果而取得的．

关于 $\zeta(s)$，还有以下重要结果：

1918 年，英国数学家哈代（G.H. Hardy）和李特伍德证明了 $\int_{-T}^{T}\left|\zeta\left(\frac{1}{2}+it\right)\right|^2dt\sim 2T\ln T$．

1926 年茵凡姆（A. E. Ingham）证明了

$$\int_{-T}^{T}\left|\zeta\left(\frac{1}{2}+it\right)\right|^4dt\sim\frac{T}{\pi^2}\ln^4T.$$

他于 1940 年又证明了当$\frac{1}{2}\leqslant\sigma<1$ 时，

$$N(\sigma,T)=O(T^{3(1-\sigma)/(2-\sigma)}\ln^5T),$$

其中 $T\geqslant 2$，$\frac{1}{2}\leqslant\alpha<1$，$N(\alpha,T)$表示$\zeta(s)$在矩形 $\alpha\leqslant\sigma<1$，

$|t|\leqslant T$ 中的零点个数，记号 O 如素数分布中所述．此结果已被不断改进．通常把这类结果称为“零点密度定理”．

黎曼首先提出用复变函数论特别是 $\zeta(s)$ 研究数论的新思想和新方法，开创了解析数论的新时期，并对单复变函数论的发展产生了深刻的影响．

6．狄利克雷特征

设 $q=2^l p_1^{l_1}\cdots p_s^{l_s}$，其中 p_j 是不同的奇素数$(1\leqslant j\leqslant s)$，$g_j$ 是模 $p_j^{l_j}(1\leqslant j\leqslant s)$的最小正原根，并且，

$$c=\begin{cases}1, & \text{当 } l=1 \text{ 时；}\\ 2, & \text{当 } l\geqslant 2 \text{ 时，}\end{cases}$$

$$c_0=\begin{cases}1, & \text{当 } l=1 \text{ 时；}\\ 2^{l-2}, & \text{当 } l\geqslant 2 \text{ 时，}\end{cases}$$

$$c_j=\varphi(p_j^{l_j}),\quad 1\leqslant j\leqslant s,$$

其中 $\varphi(d)$是不超过 d，且与 d 互素的正整数的个数．

对于任给的一组整数 m、m_0、m_1、…、m_s，把定义在整数集合上的函数

$$\chi(n)=\begin{cases}\exp\left(2\pi i\left(\dfrac{mr}{c}+\dfrac{m_0r_0}{c_0}+\dfrac{m_1r_1}{c_1}+\cdots+\dfrac{m_sr_s}{c_s}\right)\right), & \\ \qquad\qquad \text{当}(n,\ q)=1 \text{ 时；} & \\ 0, \qquad\quad \text{当}(n,\ q)>1 \text{ 时} & \end{cases}$$

称为模 q 的特征，其中 $r, r_0, r_1, \cdots, r_s$ 是 n 对模 q 的一个指数组，即 $n\equiv(-1)^r5^{r_0}\ (\mathrm{mod}\ 2^l)$，$n\equiv g_j^{r_j}(\mathrm{mod}\ p_j^{l_j})$，$1\leqslant j\leqslant s$．

为了着重指出特征 $\chi(n)$ 是属于模 q 的特征，经常

采用记号 $\chi_q(n)$或 $\chi(n)\bmod q$.

特征这一概念是数论中的重要概念之一，是狄利克雷所引进的,所以通常称为“狄利克雷特征”.它可以用不同的方法来定义,上面只是一种定义方法.

设 $\chi(n)$ 是模 q 的特征，如果当$(n, q)=1$ 时恒有 $\chi(n)=1$,则称 $\chi(n)$为“模 q 的**主特征**”,记为 $\chi^0(n)$；不然,就称为“非主特征”. 只取实值的特征称为**实特征**,其它的称为**复特征**. 函数 $\bar{\chi}(n)=\overline{\chi(n)}$也是模 q 的特征,称为 $\chi(n)$的**共轭特征**.

可以证明,模 q 的特征具有下列性质：

(1) 模 q 的特征是以 q 为周期的周期函数,即

$$\chi(n+q)=\chi(n).$$

此外，$\chi(1)=1$,$|\chi(n)|=1$，$(n, q)=1$.

(2) 特征 $\chi(n)$是完全积性函数，即对任意整数 n_1、n_2,有 $\chi(n_1, n_2)=\chi(n_1)\chi(n_2)$. 因此，$\chi^2(-1)=1$.

(3) 对于一个固定的模 q,有且仅有 $\varphi(q)$个不同的模 q 的特征.

(4) 设 $\chi(n)$是模 q 的特征,则有

$$\sum_{n=1}^{q}\chi(n)=\begin{cases}\varphi(q), & \text{当 } \chi=\chi^0 \text{ 时；}\\ 0, & \text{当 } \chi\neq\chi^0 \text{ 时.}\end{cases}$$

(5) 设 $q\geqslant 1$，$(a, q)=1$,则有

$$\sum_{\chi \bmod q}\bar{\chi}(a)\chi(n)=\begin{cases}\phi(q), & \text{当 } n\equiv a(\bmod q)\text{时；}\\ 0, & \text{当 } n\not\equiv a(\bmod q)\text{时.}\end{cases}$$

其中 $\sum\limits_{\chi \bmod q}$ 表示对模 q 的所有不同的特征求和.

(6) 设 $\chi(n)$ 是模 q 的非主特征，如果存在正整数

$q'<q$，使得对所有满足条件 $(n_1, q)=(n_2, q)=1$、$n_1\equiv n_2 \pmod{q'}$ 的 n_1、n_2，有 $\chi(n_1)=\chi(n_2)$，那么就称 $\chi(n)$ 为“模 q **的非原特征**”；否则就称为“模 q **的原特征**”.

利用上面的性质 (5)，可以从一个给定的整数序列中，把属于某个公差为 q 的算术级数的子序列分离出来. 因此，它在涉及算术级数的许多数论问题(诸如算术级数中的素数定理，哥德巴赫猜想)的研究中，起着关键的作用.

7. 狄利克雷 L 函数

狄利克雷在研究算术级数中的素数分布问题时，还引进了一个类似于黎曼 ζ 函数的复变函数，此即“对应于模 q 的特征 $\chi(n)$的狄利克雷 L 函数”，即函数

$$L(s, \chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}, \tag{40}$$

其中 $q\geqslant 1$，$\chi(n)$是模 q 的一个特征，复变数 $s=\sigma+it$，$\sigma>1$.

在 $q=1$ 时 $L(s,\chi)$就是黎曼 ζ 函数. 这类函数的性质和作用，都与黎曼 ζ 函数类似，在许多数论问题中有重要应用. 它的主要性质有：

(1) 当 $\sigma>1$ 时，$L(s,\chi)=\prod_p(1-\chi(p)p^{-s})^{-1}$，其中 $\prod_p$ 表示对全体素数求积. 因而 $L(s, \chi)\neq 0, \sigma>1$.

(2) 当 χ^0 是模 q 的主特征时，

$$L(s, \chi^0)=\zeta(s)\prod_{p|q}(1-p^{-s}), \quad \sigma>1.$$

于是，通过 $\zeta(s)$，就把 $L(s,\ \chi^0)$解析开拓到全平面.

(3) 当 χ 是模 q 的非主特征时，一定存在唯一的一个模 q^*的原特征 χ^*，使当 $\sigma>1$ 时有

$$L(s,\ \chi)=L(s,\ \chi^*)\prod_{p\mid q}(1-\chi^*(p)\ p^{-s}).$$

(4) 当 χ 是模 q 的原特征时，$L(s,\chi)$可解析开拓为整函数，且满足函数方程

$$L(1-s,\chi)=2^{1-s}\pi^{-s}\cdot q^{s-1}\tau(\chi)\Gamma(s)\cos\frac{\pi(s-a)}{2}L(s,\bar{\chi}),$$

其中 $a=a(\chi)=\frac{1}{2}(1-\chi(-1))$，$\tau(\chi)$ 为仅与 χ 有关的常数，且满足$|\tau(\chi)|=\sqrt{q}$，$\bar{\chi}$ 表 χ 的共轭特征，即 $\bar{\chi}(n)=\overline{\chi(n)}$.

(5) 对任意的模 q 的特征 χ，有 $L(1,\ \chi)\neq 0$.

(6) 设 χ 是模 q 的原特征，那么 $s=-(2n+a(\chi))$ 是 $L(s,\chi)$的一级零点($n=0,1,2,\cdots$)，称为“无聊零点”；$L(s,\ \chi)$可能有的其它零点(称为“非无聊零点”) 一定都位于带形区域 $0\leqslant\sigma\leqslant 1$ 中； $L(s,\ \chi)$确有无穷多个非无聊零点.

(7) 设 $T>0$，以 $N(T,\ \chi)$表示 $L(s,\ \chi)$在区域 $0\leqslant\sigma\leqslant 1$，$|t|\leqslant T$ 中的零点个数. 因此，当 χ 是模 q 的原特征和 $T\geqslant 2$ 时，有

$$N(T,\ \chi)=\frac{T}{\pi}\ln\frac{qT}{2\pi}-\frac{T}{\pi}+O(\ln q\,T).$$

(8) 设 $T>0$，$\frac{1}{2}\leqslant\alpha<1$，以 $N(\alpha,\ T,\ \chi)$表示 $L(s,\ \chi)$ 在区域 $\alpha\leqslant\sigma\leqslant 1$，$|t|\leqslant T$ 中的零点个数. 再设 $N(\alpha,$

$T, q) = \sum_{\chi \bmod q} N(\alpha, T, \chi)$，其中 $\sum_{\chi \bmod q}$ 表对模 q 的所有特征求和.因此，当 $T \geqslant 2$ 时有

$$N(\alpha, T, q) = O((qT)^{3(1-\alpha)/(2-\alpha)} (\ln qT)^9).$$

此结果已被改进和推广，通常称之为"L 函数的零点密度定理".

(9) 在直线 $\sigma = 1$ 上 $L(s, \chi) \neq 0$. 由此，对任意固定的 q，可推出算术级数中的素数定理.

(10) 存在绝对正常数 c_1，使得对任意固定的模 q，在所有的函数 $L(s, \chi)(\chi \bmod q)$ 中，仅可能除去一个例外函数外，均在区域 $\sigma \geqslant 1 - c_1(\ln(q|t| + 2))^{-1}$ 内无零点，如果这样的例外函数 $L(s, \tilde{\chi})$ 存在，那么 $\tilde{\chi}$ 一定是模 q 的实的非主特征，且 $L(s, \tilde{\chi})$ 在上述区域内只有一个一级实零点 $\tilde{\beta}$. 这一性质是狄利克雷 L 函数与黎曼 ζ 函数的一个主要差别. 研究对应于实特征的 L 函数的实零点，是 L 函数论的最重要问题之一.关于这方面的结果，例如：

(11) 帕吉于 1935 年证明了：存在绝对正常数 c_2，使得对任意的实原特征 $\chi \bmod q$，$q \geqslant 3$，必有 $L(1, \chi) \geqslant c_2 q^{-\frac{1}{2}}$. 由此推出，存在绝对正常数 c_3，使得对任意的实特征 $\chi \bmod q$，$q \geqslant 3$，当 $\sigma \geqslant 1 - c_3(\sqrt{q} \ln^2 q)^{-1}$ 时，$L(\sigma, \chi) \neq 0$.

(12) 塞格尔(C. L. Siegel)于 1936 年证明了：对任给的正数 ε，存在正常数 $c_3(\varepsilon)$，使得对任意的实原特征 $\chi \bmod q$，$q \geqslant 3$，必有 $L(1, \chi) \geqslant c_3(\varepsilon) q^{-\varepsilon}$. 由此推出，对

任给正数 ε，必有正常数 $c_4(\varepsilon)$，使得对任意的实特征 $\chi \bmod q$，$q \geqslant 3$，当 $\sigma \geqslant 1 - c_4(\varepsilon) q^{-\varepsilon}$ 时，$L(\sigma, \chi) \neq 0$.

塞格尔的结果虽然优于帕吉的结果，但是常数 $c_3(\varepsilon)$ 和 $c_4(\varepsilon)$ 至今没有办法计算出来.

从性质 10、11、12 可推得有余项估计的算术级数中的素数定理. 类似于黎曼假设，有所谓广义黎曼假设，即猜测所有的狄利克雷 L 函数的非无聊零点都位于直线 $\sigma = \frac{1}{2}$ 上，通常简记作 GRH. 大量的数值计算以及理论上的探讨都支持这一假设，但它至今还没有被证明或否定. 从 GRH 可推出一系列重要的数论结果，虽然都是一些假设性的结果（其中有的已被无条件地证明了），但是却指出了研究 L 函数零点的重要意义和方向.

三、代 数 数 论

前面我们曾谈到过一些不定方程，许多著名的数学家，如费马，欧拉，高斯，拉格朗日(J. L. Lagrange)，库默(E. E. Kummer)，希尔伯特(D. Hilbert)等，都从事过不定方程的研究. 希尔伯特在 1900 年提出的二十三个著名问题中，第十个问题就是问：能否判断任何整系数多项式 $f(x_1, \cdots, x_s) = 0$ 有没有整数解，这个问题直到 1970 年才得到了否定的回答. 前面我们还提到过费马在 1637 年提出了一个猜想："不可能把一个正整数的三次方幂分

成两个三次方幂的和，一个四次方幂分成两个四次方幂的和，或一般地，不可能把任一个次数大于 2 的正整数的方幂分成两个同方幂的和”.这就是众所周知的**费马大定理**. 当时，他把这个论断写在一本书的空白处，并且紧接着又写道："我发现这个论断的证明，但是书的空白太窄了，写不下."如果用不定方程来表示，费马大定理即是说：

设整数 $n \geqslant 3$，不定方程

$$x^n + y^n = z^n \tag{9}$$

除平凡解 $xyz = 0$ 外，没有其他整数解 x、y、z.

可是，费马始终没有给出这个问题的证明.估计后来他采用无穷递降法只证明了 $n = 4$ 时命题成立. 到 1753 年，欧拉证明了当 $n = 3$ 时命题成立.1823 年，当时已 71 岁的法国数学家勒让德与只有 18 岁的狄利克雷，几乎同时证明了 $n = 5$ 时命题成立. 随后不久，拉梅(G. Lamé)证明了 $n = 7$ 时的情况. 到 1849 年，德国数学家库默一下子证明了当 $2 < n \leqslant 100$ (除去 37，59，67)时，费马大定理均成立.而直到三百多年后的今天，虽经许多优秀数学家的努力，仍然没有能证明费马大定理的成立，也未能否定它. 然而，数学家们的辛勤劳动并没有白费，其中德国数学家库默为了解决费马大定理，而引进了“理想数”的概念，这为“代数数论”奠定了基础.

我们先从一个简单的例子说起. 给出一个二次不定方程

$$x^2 + y^2 = z^2, \tag{5}$$

要求出它的全部整数解.

显然,若$(x,y)=d>1$,则可得$d^2|z^2$, $d|z$.于是可将(5)式两边约去d^2,因此可以设$(x,y)=1$.同时,只需求$x>0$, $y>0$, $z>0$的整数解,并且x和y不能同为奇数,否则(5)式取模4便有

$$z^2\equiv 2(\bmod 4),$$

而这是不可能的.因此,对(5)式的解,经上面的简化之后,有:不定方程(5)式满足

$$(x,y)=1,\quad x>0,\ y>0,\ z>0,\ 2|x$$

的全部整数解,可表为

$$x=2ab,\qquad y=a^2-b^2,\qquad z=a^2+b^2,\tag{8}$$

其中$a>b>0$, a、b为一奇一偶,且满足$(a,b)=1$的任意整数.

如果我们把整数的范围扩大,考虑所有实部和虚部都取整数的复数,则(5)式的左边可分解为$x^2+y^2=(x+yi)(x-yi)$.这样,方程(5)式就变得容易解决了.

用$\mathbf{Z}$表示全体整数所成的集合,则全体实部与虚部皆取整数的复数可表为:

$$\mathbf{Z}(i)=\{a+bi\mid a、b\in\mathbf{Z}\}.$$

显然,当$b=0$时,$\mathbf{Z}(i)$里的数就是有理整数了,因此$\mathbf{Z}\subset\mathbf{Z}(i)$.我们称$\mathbf{Z}(i)$中的复数为复整数.若记$\mathbf{Q}$是全体有理数所成的集合,则全体实部和虚部都取有理数的复数可记为:

$$\mathbf{Q}(i)=\{\alpha+\beta i\mid \alpha、\beta\in\mathbf{Q}\}.$$

对于复数的加法与乘法,$\mathbf{Q}(i)$组成一个数域,通常把

Q(i)称为是 i 添加到 **Q** 上的代数数域.

下面我们将引进复整数的整除、素数等概念.

设复整数 η、$\xi\neq0$,若存在复整数 ζ,使

$$\eta=\xi\zeta, \tag{41}$$

则称 ξ **整除** η,记为 $\xi|\eta$; 否则,称 ξ **不整除** η,记为 $\xi\nmid\eta$.

在有理整数（为区别通常的整数与其他数域中的整数,把通常的整数称为有理整数)中，整除 1 的整数仅有 ±1. 在复整数中，整除 1 的有 ±1、$\pm i$，这四个数称为 **Q**(i)的**单位数**.令 $\xi=a+bi$,其共轭复数便是 $\overline{\xi}=a-bi$，我们把 $N(\xi)=\xi\overline{\xi}=a^2+b^2$ 叫做 ξ 的**范数**. 又，设 ε 为 $Q(i)$的单位数，若复整数 ξ、η 满足 $\xi=\eta\varepsilon$，则称 $\overline{\xi}$ 与 η **相结合**. 当 $N(\xi)=1$ 时，若任何分解式 $\xi=\eta p$，都有 $N(\eta)=1$ 或 $N(p)=1$,则称 ξ 是 **Q**(i)的**素数**,常用 π 表示. 可以证明 **Q**(i)中的素数是：$1+i$ 和它的相结合数、有理素数 p(这里 $p\equiv3(\bmod 4)$)和它的相结合数、有理素数 q(这里 $q\equiv1(\bmod 4)$)的因数 $a+bi$.

与有理整数相类似，可以证明复整数的唯一分解定理是成立的,即:设 $N(\xi)>1$,若有

$$\xi=\pi_1\cdots\pi_r=\pi_1'\cdots\pi_s' \text{（其中 } s\geqslant1,\ r\geqslant1\text{)},$$

则有 $r=s$,且若不计 π 与 π' 的次序，则诸 π 分别是诸 π'的相结合数.

但是,把$\sqrt{-5}$添加到 **Q** 上得到的数域 **Q**$(\sqrt{-5})$里，虽然可类似地定义其整数、范数、相结合、素数等概念,遗憾的是唯一分解定理却不成立.例如

$$6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

可以验证 $2,3,1+\sqrt{-5},1-\sqrt{-5}$ 皆为 $\mathbf{Q}(\sqrt{-5})$ 中的素数，且 2,3 不能与 $1+\sqrt{-5},1-\sqrt{-5}$ 相结合，故 6 的分解式不唯一.

我们把系数是有理数的 n 次不可约多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

的根 θ，称为“n 次代数数”．若 n 次不可约多项式的首项系数 $a_n=1$，其余系数为有理整数，则其根 θ 称为“**n 次代数整数**”

将一个 n 次代数整数 θ 添加到有理数域 $\mathbf{Q}$ 上，则可得到一个 n 次代数数域 $\mathbf{Q}(\theta)$．$\mathbf{Q}(\theta)$ 中任一数 α 均可表为

$$\alpha=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1},\ \text{其中}\ a_i\in\mathbf{Q},\ i=0,1,\cdots,n-1.$$

记 $\theta=\theta^{(1)}$，并设 $\theta^{(2)},\cdots,\theta^{(n)}$ 为 θ 所适合的不可约多项式的其他 $n-1$ 个根．再设 $\alpha^{(1)}=\alpha$，则称

$$\alpha^{(k)}=a_0+a_1\theta^{(k)}+\cdots+a_{n-1}\theta^{(k)n-1}\qquad(k=2,3,\cdots,n)$$

为 α 的**共轭数**．又，称

$$N(\alpha)=\alpha^{(1)}\cdots\alpha^{(n)}$$

为 α 的**范数**.

设 α 是 $\mathbf{Q}(\theta)$ 中的一个代数整数，若 α^{-1} 也是代数整数，则称 α 为 $\mathbf{Q}(\theta)$的**单位数**．易知，代数整数 α 为单位数的充要条件是 $N(\alpha)=\pm 1$．设 $\omega_1,\cdots,\omega_m$ 为 $\mathbf{Q}(\theta)$ 中的 m 个代数整数，若 $\mathbf{Q}(\theta)$中的任一代数整数都能唯一地表为

$$a_1\omega_1+\cdots+a_m\omega_m,\qquad(a_i\in\mathbf{Z},\ i=1,\cdots,m)$$

则称 $\omega_1, \cdots, \omega_m$ 是 $\mathbf{Q}(\theta)$的一组**整基底**,也简称为**整底**.

设 α、β 是 $\mathbf{Q}(\theta)$中两个代数整数，若有一代数整数 γ,使 $\alpha=\beta\gamma$,则称 β **可整除** α,记为 $\beta|\alpha$;否则，称 β 不能整除 α,记为 $\beta\nmid\alpha$. 若两个代数整数 α、β 仅相差一个单位因子,则 α 与 β 称为**相结合**.

设 α 是非单位数又非 0 的代数整数,如果有 $\mathbf{Q}(\theta)$的非单位数的代数整数 β、γ.使 $\alpha=\beta\gamma$,则称 α 在 $\mathbf{Q}(\theta)$ 中**可分解**;否则,称 α 是 $\mathbf{Q}(\theta)$中的**素数**. 虽然 $\mathbf{Q}(\theta)$中的任一非单位数 α (这里 $\alpha\neq0$)可分解为素数的乘积,但一般的代数数域中分解是不唯一的.为了使分解式能唯一,库默引进了理想数:

设 $\alpha_1, \cdots, \alpha_q$ 为 $\mathbf{Q}(\theta)$内任意 q 个代数整数,称所有形如

$$\eta_1\alpha_1+\cdots+\eta_q\alpha_q \tag{42}$$

(其中 $\eta_1, \cdots, \eta_q$ 为 $\mathbf{Q}(\theta)$ 中的整数) 的代数整数组成的集,为由 $\alpha_1, \cdots, \alpha_q$ 生成的**理想数**,以$[\alpha_1, \cdots, \alpha_q]$表示.

设 $A=[\alpha_1, \cdots, \alpha_q]$、$B=[\beta_1, \cdots, \beta_r]$,定义

$$AB=[\alpha_1\beta_1, \cdots, \alpha_1\beta_r, \cdots, \alpha_q\beta_1, \cdots, \alpha_q\beta_r]. \tag{43}$$

若一理想数除了单位理想数[1]和本身以外,无其他因子,则称为**素理想数**.只由一个代数整数 α 生成的理想数$[\alpha]$称为**主理想**.

对于理想数,唯一分解定理成立.即任一不同于单位理想[1]和[0]的理想数 A,可以分解为素理想数的乘积,且如果不计其排列的次序,分解式的表示法是唯一的.

设 α、β 是 $\mathbf{Q}(\theta)$中的代数整数,若 $A|(\alpha-\beta)$, 则称

α和β对模 A 同余，记为

$$\alpha \equiv \beta (\bmod A). \tag{44}$$

于是，由同余关系式可将域 $\mathbf{Q}(\theta)$的全体代数整数按模A进行分类，其类数是有限的，记为 $N(A)$，称为理想数 A 的范数，且有

$$N(AB) = N(A)N(B). \tag{45}$$

设 A、B 是 $\mathbf{Q}(\theta)$上的理想数，如果有 $\mathbf{Q}(\theta)$上的主理想数$[\alpha]$和$[\beta]$，使

$$[\alpha]A = [\beta]B$$

成立，称 A 和 B “属于同一理想”，记为 $A \sim B$. 这样我们可将 $\mathbf{Q}(\theta)$ 上的全体理想数进行分类，称为理想数类，其类数也有限，记为 h.

设 A 是 $\mathbf{Q}(\theta)$上任一个理想数，则总存在 $\mathbf{Q}(\theta)$ 中的一个代数整数 β，使

$$A^h = [\beta]$$

成立. 由此可知，若 A^l 是一个主理想数，且有$(l, h) = 1$，则 A 是一个主理想数$[\alpha]$.

在一般代数数域$\mathbf{Q}(\theta)$中，最常用到的是所谓二次域 $\mathbf{Q}(\sqrt{d})$，其中 d 为一个无平方因子的有理整数.

由于库默引进了“理想”的概念，代数数论得到了极大的发展. 尤其在不定方程的研究中，理想数的出现，使这一数学分支的许多困难得以克服. 正如前面所提到的，库默自己就成功地证明了当 $n \leqslant 100$时费马大定理成立. 在此基础上，人们进一步研究，陆续得到了一些新的进展. 目前，对于小于 10^5 的所有素数 p，已证明了费马大

定理 决于对素数 p 来判断其正确与

诸如理 数论中的概念，其意义早已远远超出了“数论”的范围.

*　　*　　*　　*　　*

此外，由闵科夫斯基和沃洛诺伊奠基的几何数论，所研究的基本对象是“空中格网”，也就是全部“整点”的组，而“整点”是指给定的直线坐标系统内坐标全是整数的点.空间格网对几何学和结晶学有巨大的意义.计算在给定区域中整点数目的方法，对许多物理学部门也是非常重要的.

需说明的是，我们在这里仅介绍了数论中的一部分基本概念；在众多的世界著名数论问题中，我们也只是简单地谈论了其中的几个问题. 有志于数论工作的读者，以及想对数论学科作全面深入了解的读者，应该去读众多的国内、外数论专著，尤其是我国著名数学家华罗庚教授的《数论导引》一书.